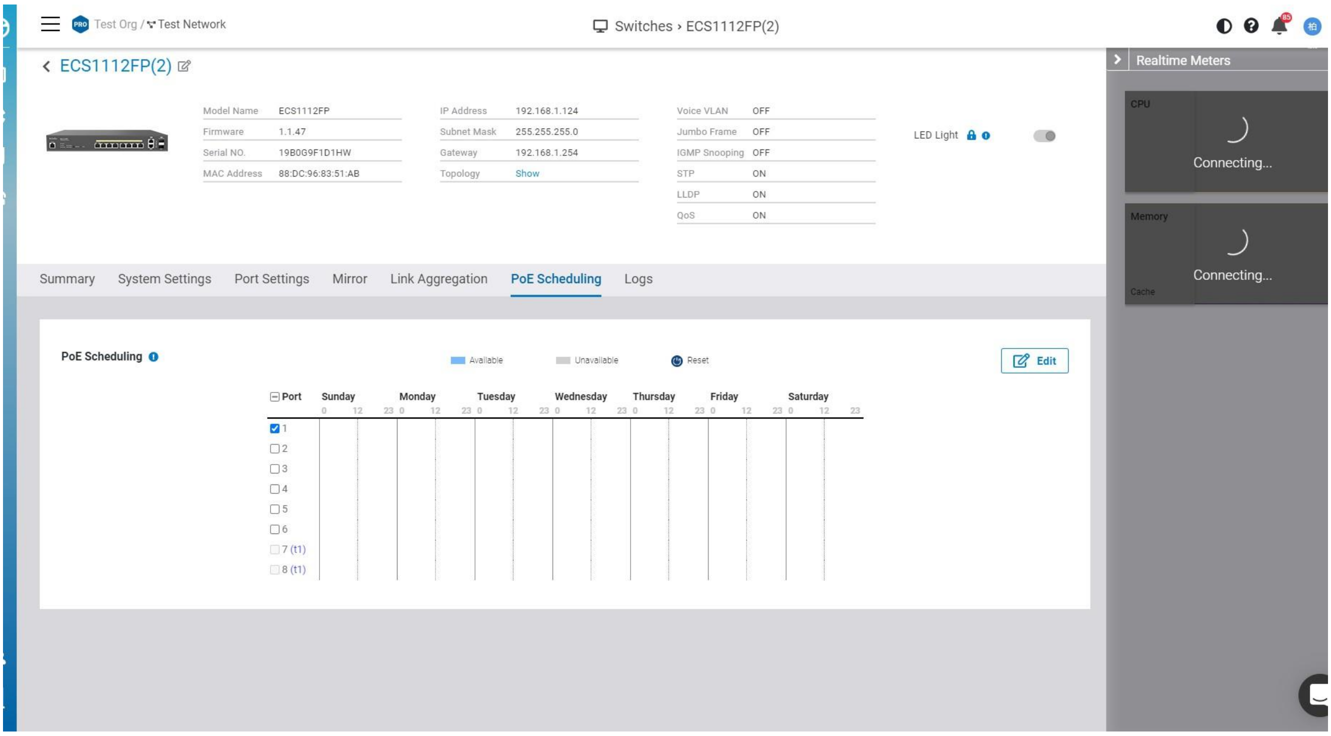
# Edit PoE Scheduling

1. Select the ports to be set the PoE scheduling then click Edit



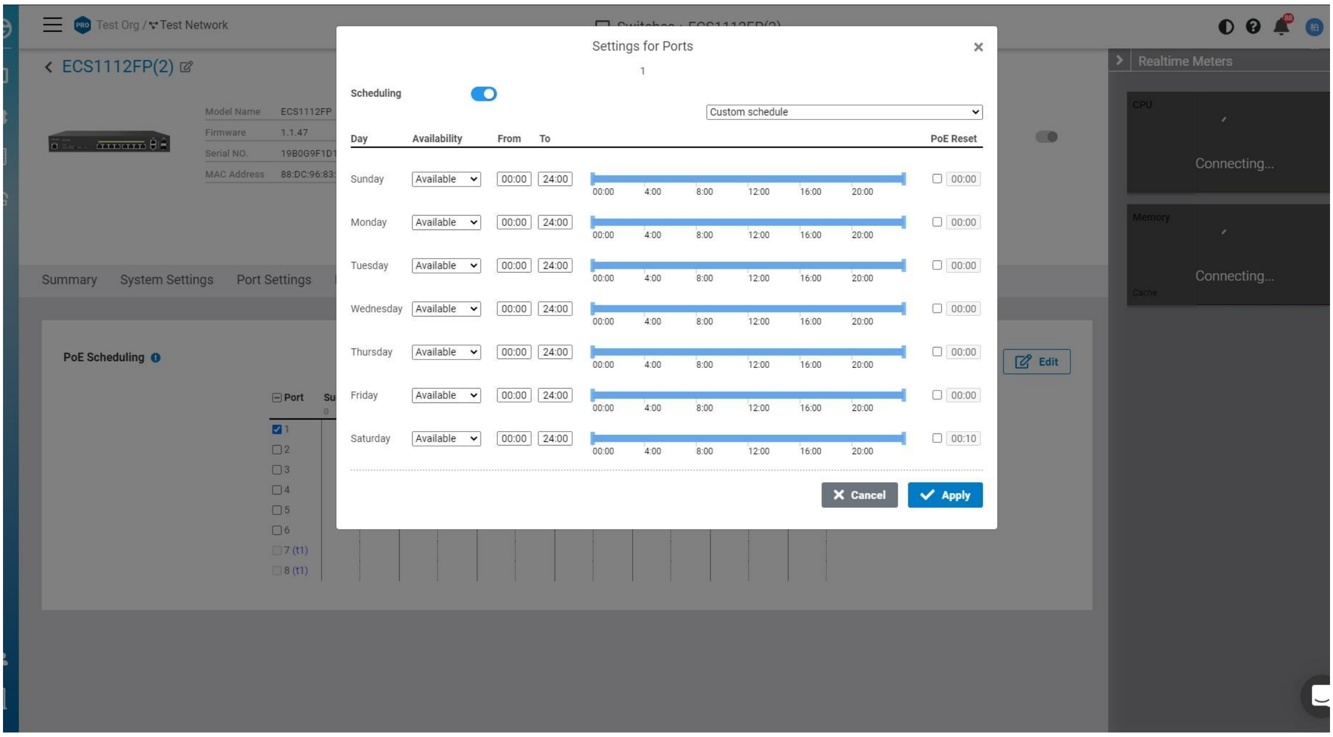
| | | | | | |
|---|---|---|---|---|---|
| Model Name | ECS1112FP | IP Address | 192.168.1.124 | Voice VLAN | OFF |
| Firmware | 1.1.47 | Subnet Mask | 255.255.255.0 | Jumbo Frame | OFF |
| Serial NO. | 19B0G9F1D1HW | Gateway | 192.168.1.254 | IGMP Snooping | OFF |
| MAC Address | 88:DC:96:83:51:AB | Topology | Show | STP | ON |
| | | | | LLDP | ON |
| | | | | QoS | ON |

LED Light

PoE Scheduling

| Port | Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday |
|---|---|---|---|---|---|---|---|
| ☑ 1 | | | | | | | |
| □ 2 | | | | | | | |
| □ 3 | | | | | | | |
| □ 4 | | | | | | | |
| □ 5 | | | | | | | |
| □ 6 | | | | | | | |
| □ 7 (t1) | | | | | | | |
| □ 8 (t1) | | | | | | | |

2. Enable scheduling and then customize the PoE on or Off by dragging the bar. This behavior is the same when you configure the SSID scheduling.



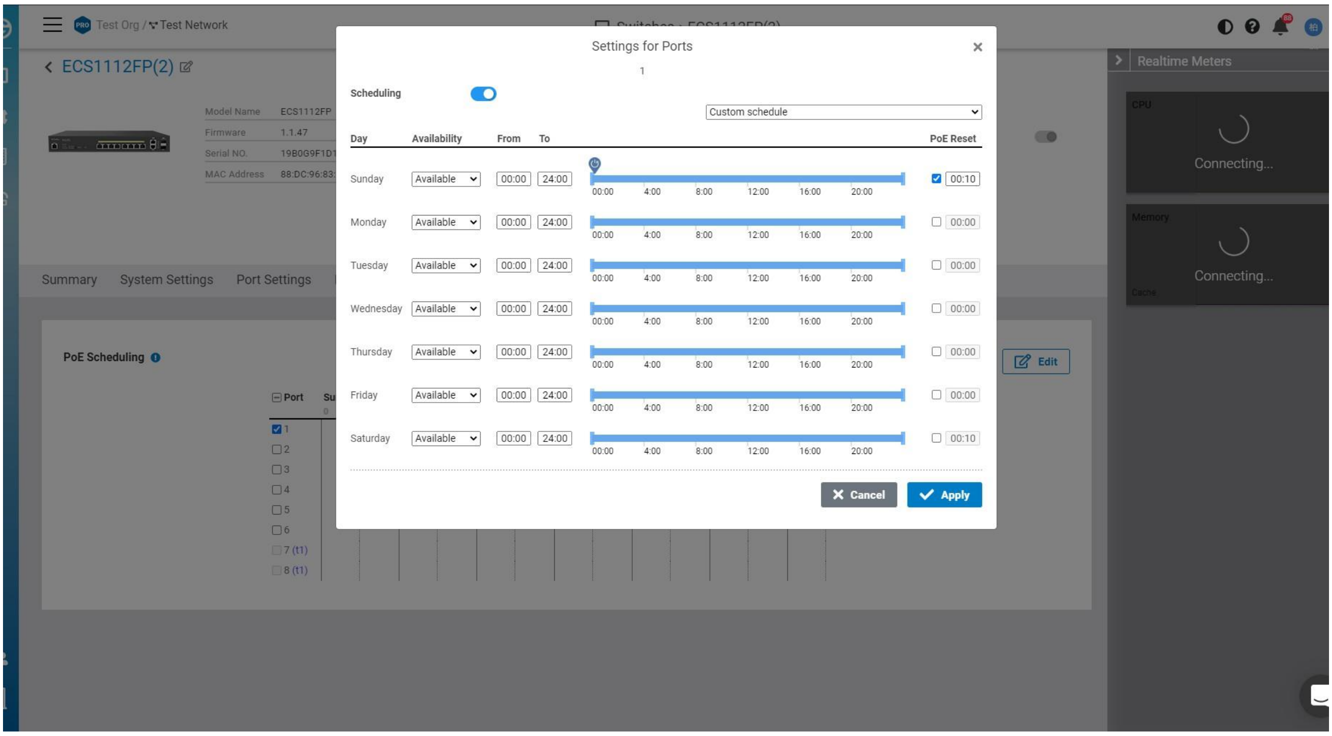
Settings for Ports

1

Scheduling ●

Custom schedule

| Day | Availability | From | To | PoE Reset |
|---|---|---|---|---|
| Sunday | Available | 00:00 | 24:00 | □ 00:00 |
| Monday | Available | 00:00 | 24:00 | □ 00:00 |
| Tuesday | Available | 00:00 | 24:00 | □ 00:00 |
| Wednesday | Available | 00:00 | 24:00 | □ 00:00 |
| Thursday | Available | 00:00 | 24:00 | □ 00:00 |
| Friday | Available | 00:00 | 24:00 | □ 00:00 |
| Saturday | Available | 00:00 | 24:00 | □ 00:10 |

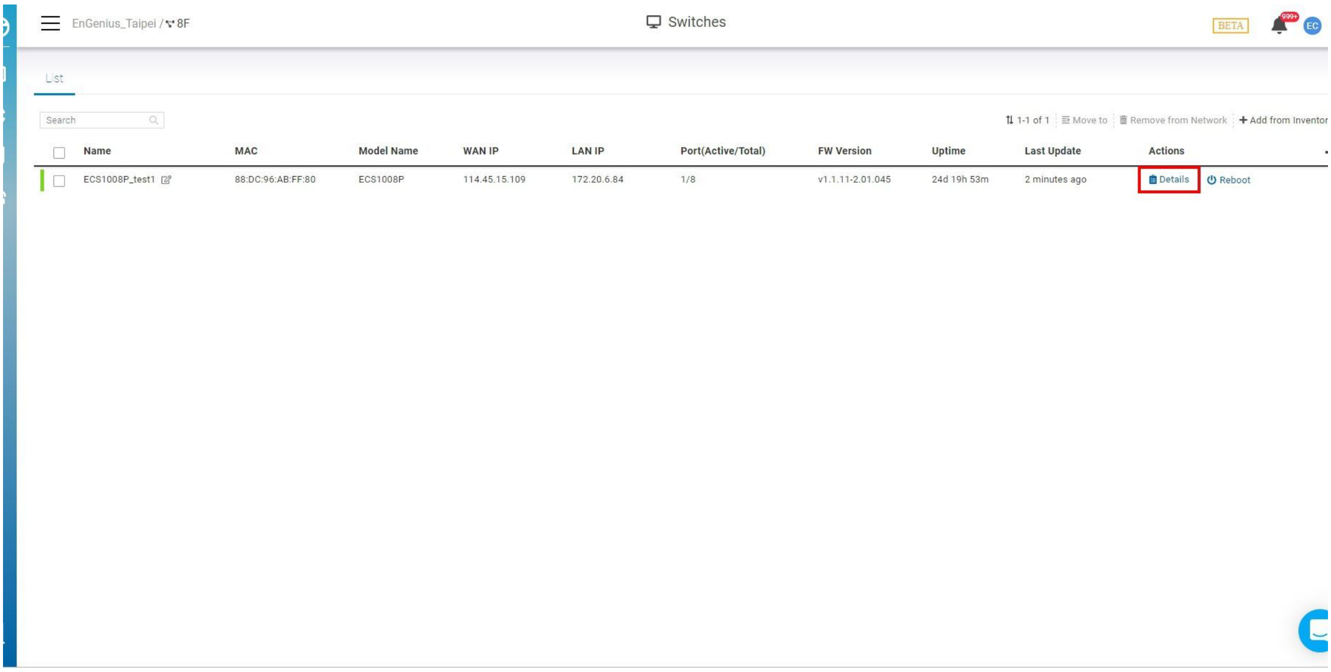


| Day | Availability | From | To | PoE Reset |
|---|---|---|---|---|
| Sunday | Available | 00:00 | 24:00 | ☑ 00:10 |
| Monday | Available | 00:00 | 24:00 | □ 00:00 |
| Tuesday | Available | 00:00 | 24:00 | □ 00:00 |
| Wednesday | Available | 00:00 | 24:00 | □ 00:00 |
| Thursday | Available | 00:00 | 24:00 | □ 00:00 |
| Friday | Available | 00:00 | 24:00 | □ 00:00 |
| Saturday | Available | 00:00 | 24:00 | □ 00:10 |

4. Click Apply.

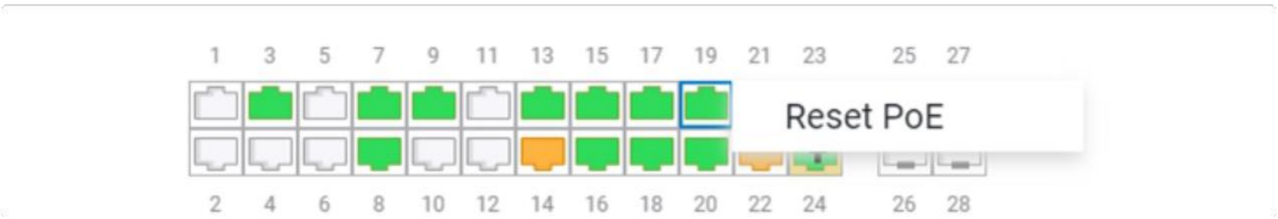
## Getting Switch Analytics

From the **Switches** page, you can click **Details** on the web interface to display detailed information about a switch.



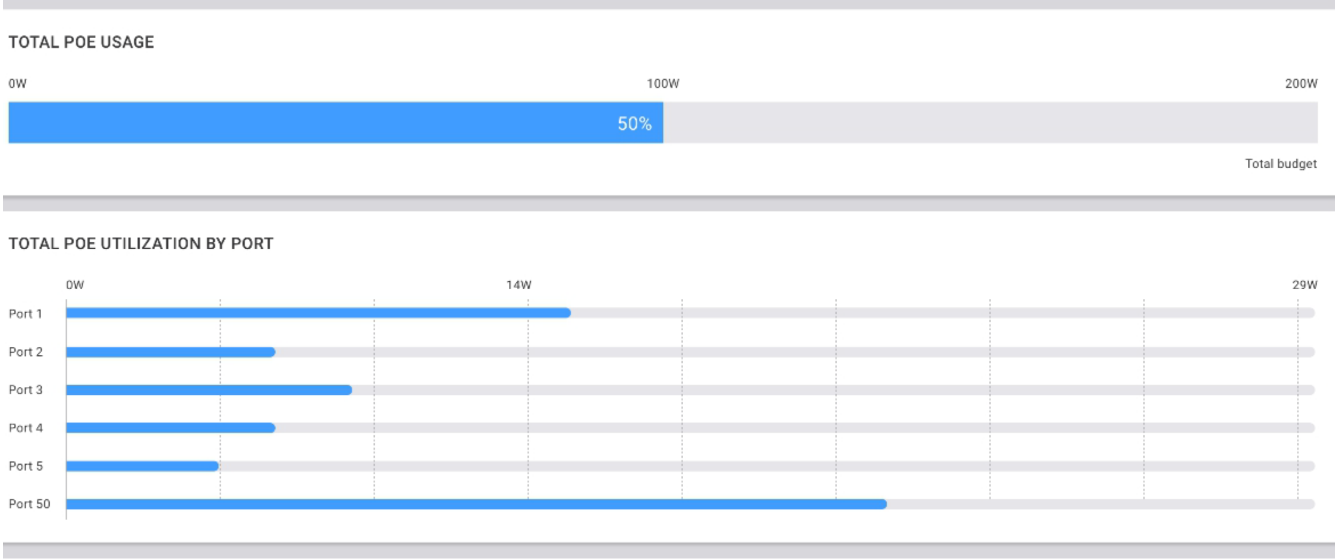
| □ | Name | MAC | Model Name | WAN IP | LAN IP | Port(Active/Total) | FW Version | Uptime | Last Update | Actions |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | ECS1008P_test1 | 88:DC:96:AB:FF:80 | ECS1008P | 114.45.15.109 | 172.20.6.84 | 1/8 | v1.1.11-2.01.045 | 24d 19h 53m | 2 minutes ago | Details Reboot |

**PoE reset from the Switch Panel :**
User can mouse-over to the PoE port of the switch port panel and power-cycle the port, so the device attached to the port will be rebooted



**Total PoE Usage:** This bar graph displays the consumed, remaining, and total wattage utilized by Power over Ethernet.

**Total PoE Utilization by Port:** Displays the current PoE utilization by each port, in watts.

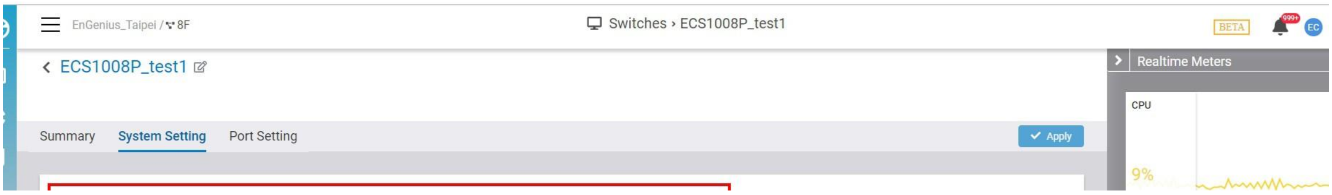


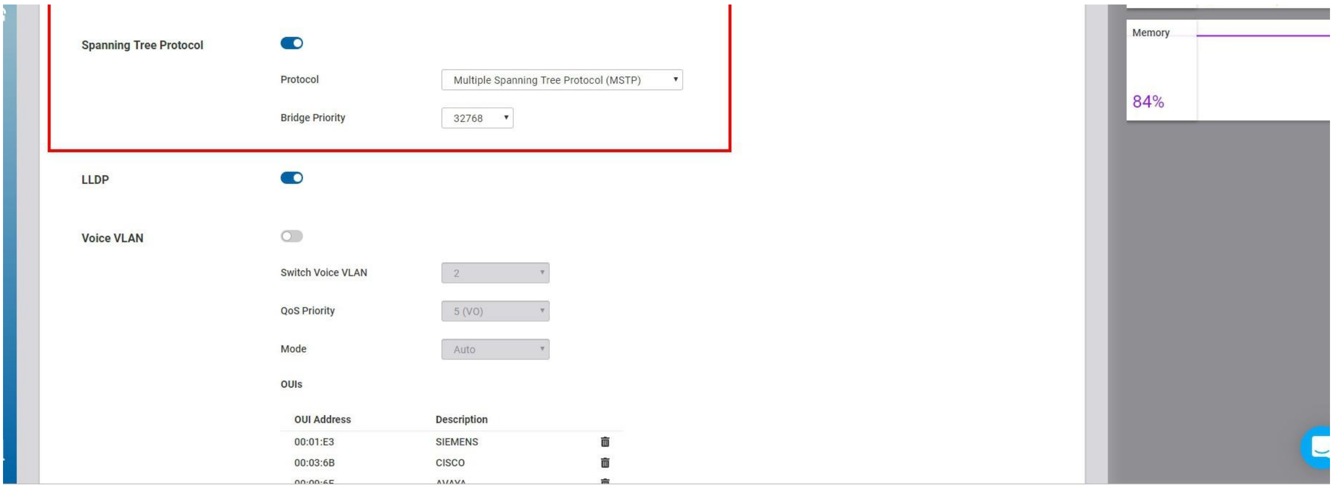
# System Setting

The System Settings section allows you to configure all primary networking options for your switch.

## Spanning Tree Protocol

A **Spanning Tree Protocol** is a Layer 2 protocol that prevents loops in a network with redundant paths created by multiple switches. We recommend using this feature if your environment incorporates multiple switches.





Spanning Tree Protocol

Protocol: Multiple Spanning Tree Protocol (MSTP)

Bridge Priority: 32768

LLDP

Voice VLAN

Switch Voice VLAN: 2

QoS Priority: 5 (VO)

Mode: Auto

OUIs

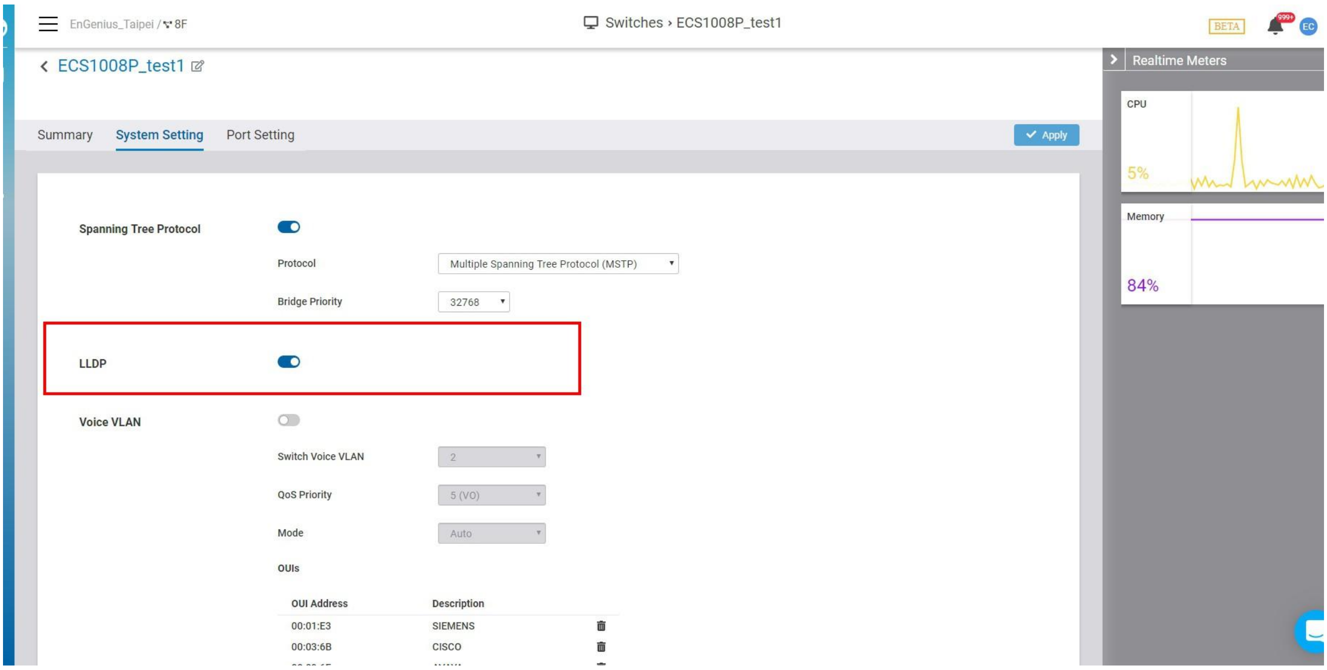
| OUI Address | Description |
|---|---|
| 00:01:E3 | SIEMENS |
| 00:03:6B | CISCO |
| 00:09:6E | AVAYA |

Procedure

1. **Enable** the **STP** option
2. Select a **Protocol**
3. Select a **Bridge Priority** value
4. Click **Apply**

## LLDP

The **Link Layer Discovery Protocol (LLDP)** is a Layer 2, vendor-neutral protocol that allows network devices to advertise capabilities, identity, and other information. This data can potentially be queried by SNMP.



Spanning Tree Protocol

Protocol: Multiple Spanning Tree Protocol (MSTP)

Bridge Priority: 32768

LLDP

Voice VLAN

Switch Voice VLAN: 2

QoS Priority: 5 (VO)

Mode: Auto

OUIs

| OUI Address | Description |
|---|---|
| 00:01:E3 | SIEMENS |
| 00:03:6B | CISCO |

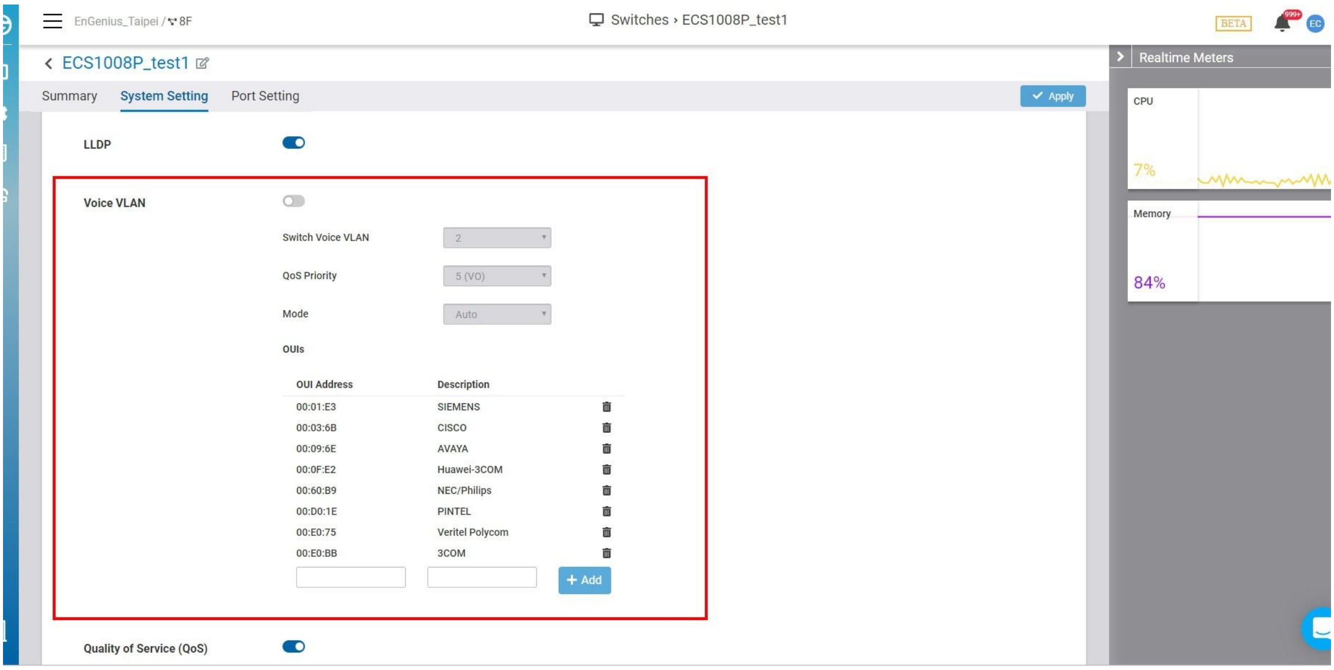
Procedure

1. **Enable** the **LLDP** option

2. Click **Apply**

### Voice VLAN

The **Voice VLAN** feature configures switches to automatically allow and prioritize voice traffic over a designated VLAN. This keeps voice traffic separate and prioritized over other traffic types.



LLDP: on

Voice VLAN: off

Switch Voice VLAN: 2

QoS Priority: 5 (VO)

Mode: Auto

OUIs

| OUI Address | Description |
|---|---|
| 00:01:E3 | SIEMENS |
| 00:03:6B | CISCO |
| 00:09:6E | AVAYA |
| 00:0F:E2 | Huawei-3COM |
| 00:60:B9 | NEC/Philips |
| 00:D0:1E | PINTEL |
| 00:E0:75 | Veritel Polycom |
| 00:E0:BB | 3COM |

Quality of Service (QoS): on

**Mode:** Allows you to define the Voice VLAN mode.

- **Auto**: Automatically advertises the Voice VLAN to connected devices via the LLDP-MED protocol.
- **OUIs**:  Determines whether a received packet is a voice packet by checking its source MAC address.

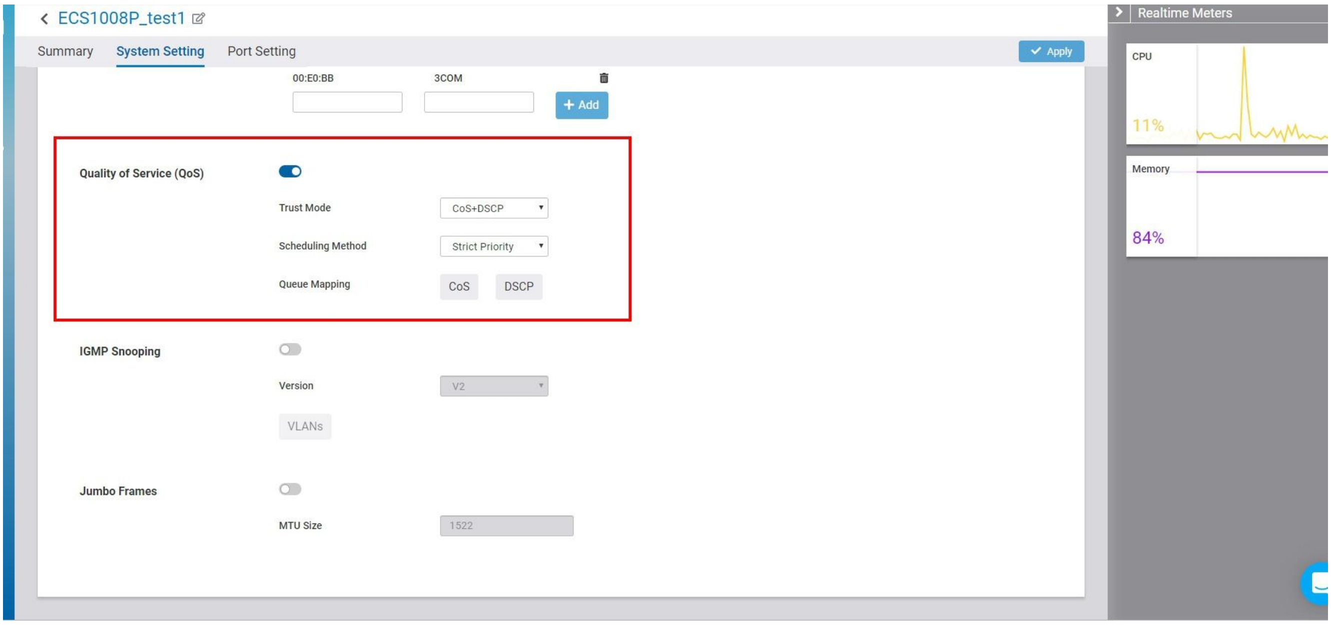
**Switch Voice VLAN**: Allows you to choose what VLAN is used for Voice VLAN. You can set up VLANs in Port Settings.

**QoS Priority:** Lets you define whether the switch will use the Quality of Service CoS value of the incoming packet, or tag the packet with a CoS value between 1-7.

**OUIs:** VoIP traffic has a pre-configured Organizationally Unique Identifier (OUI) prefix in the source MAC address. You can manually add a specific manufacturer's MAC address and description to the OUI table. All traffic received on the Voice VLAN ports from the specific IP phone with a listed OUI is forwarded on the voice VLAN.

### QoS

Quality of service (QoS) allows operators to prioritize application traffic to ensure that latency-affected data, such as VoIP and video conferencing, is uninterrupted during periods of network congestion. Switches implement this by reading tagged packets and prioritizing them accordingly. Packets are classified using **Class of Service (CoS)** on the data link layer, and **Differentiated Services Code Points (DSCP)** on the network layer, mapped to a queue, then sent out accordingly as per QoS.



| 00:E0:BB | 3COM |
|---|---|

Quality of Service (QoS): ●

Trust Mode: CoS+DSCP

Scheduling Method: Strict Priority

Queue Mapping: CoS DSCP

IGMP Snooping: ○

Version: V2

VLANs

Jumbo Frames: ○

MTU Size: 1522

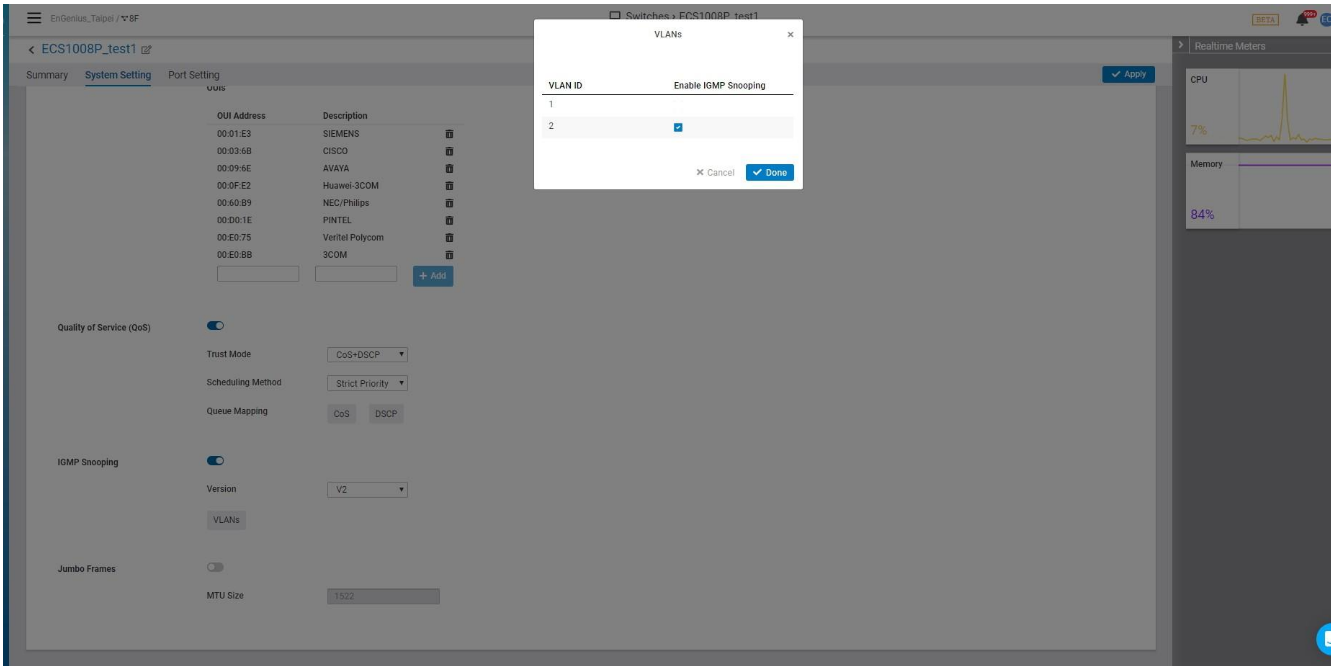
**Trust Mode:** Allows you to define whether the switch will use CoS, DSCP, or both trust modes for QoS.

**Scheduling Method:** Allows you to define what method the switch will use when assessing transmitting incoming packets in queues. **Strict priority** always prioritizes queues with a higher priority, while **Weighted Round Robin (WRR)** weights each queue by priority, then applies a round-robin policy when choosing packets for transmission.

**Queue Mapping:** Tagged packets are sent to queues defined in this setting. For each CoS or DSCP value, you can choose the queue to which tagged packets are mapped.

## IGMP

**IGMP Snooping** is used for controlling multicast traffic. It listens to IGMP messages being processed by the switch and prevents these messages from being sent to hosts not part of the respective multicast.



OUIs

| OUI Address | Description |
|---|---|
| 00:01:E3 | SIEMENS |
| 00:03:6B | CISCO |
| 00:09:6E | AVAYA |
| 00:0F:E2 | Huawei-3COM |
| 00:60:B9 | NEC/Philips |
| 00:D0:1E | PINTEL |
| 00:E0:75 | Veritel Polycom |
| 00:E0:BB | 3COM |

VLANs

| VLAN ID | Enable IGMP Snooping |
|---|---|
| 1 | □ |
| 2 | ☑ |

Quality of Service (QoS): ●

Trust Mode: CoS+DSCP

Scheduling Method: Strict Priority

Queue Mapping: CoS DSCP

IGMP Snooping: ●

Version: V2

VLANs

Jumbo Frames: ○

MTU Size: 1522

**Version:** The available IGMP Snooping versions are v2 and v3. You can select either/or in the **Version**

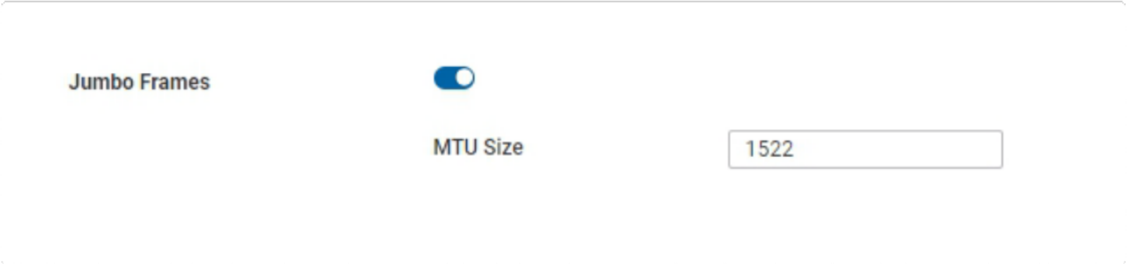
dropdown
**VLANS:** You can enable IGMP Snooping for any VLAN by selecting the corresponding checkbox next to the VLAN ID.

### Jumbo Frame

Ethernet has used the 1500 byte frame size since its inception. Jumbo frames are network layer PDUs that have a size much larger than the typical 1500 byte Ethernet Maximum Transmission Unit (MTU) size. Jumbo frames extend Ethernet to 9000 bytes, making them large enough to carry an 8 KB application datagram plus packet header overhead. If you intend to leave the local area network at high speeds, the dynamics of TCP will require you to use large frame sizes.

The switch supports a jumbo frame size of up to **9216 bytes**. Jumbo frames need to be configured to work on the ingress and egress port of each device along the end-to-end transmission path. Furthermore, all devices in the network must also be consistent on the maximum jumbo frame size, so it is important to do a thorough investigation of all your devices in the communication paths to validate their settings.

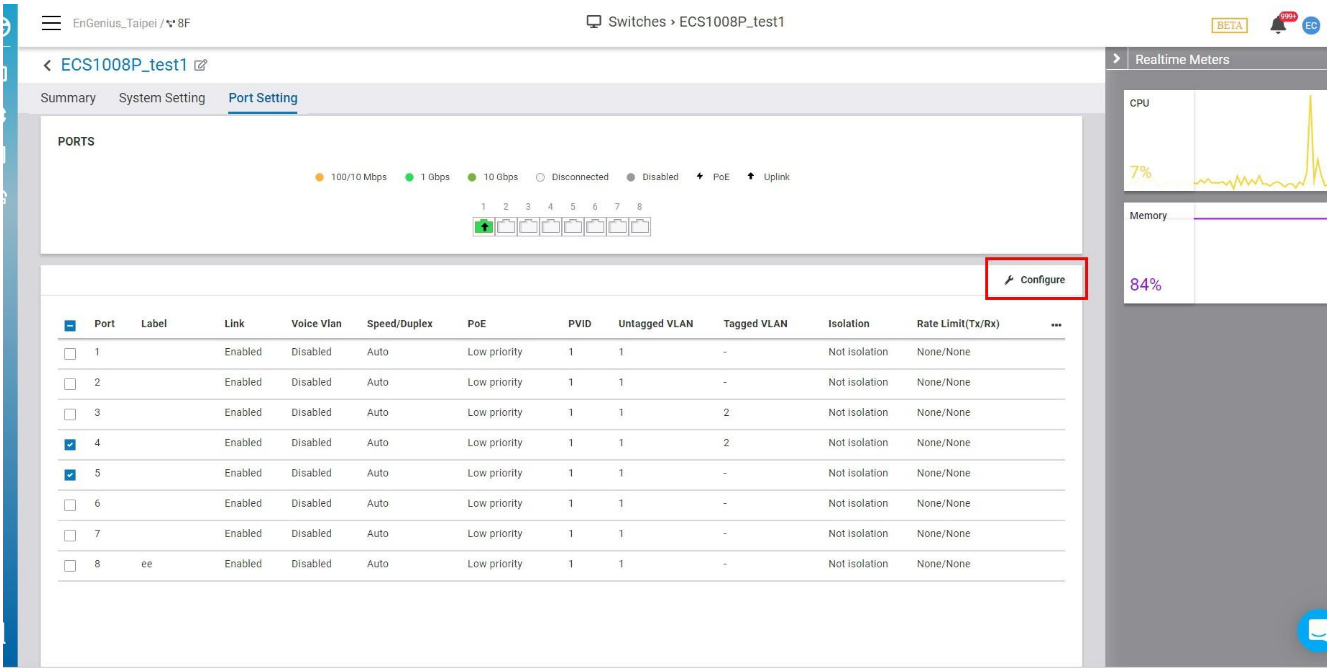
**Jumbo Frame** : Enter the size of a jumbo frame. The range is from **1522 to 9216** bytes.



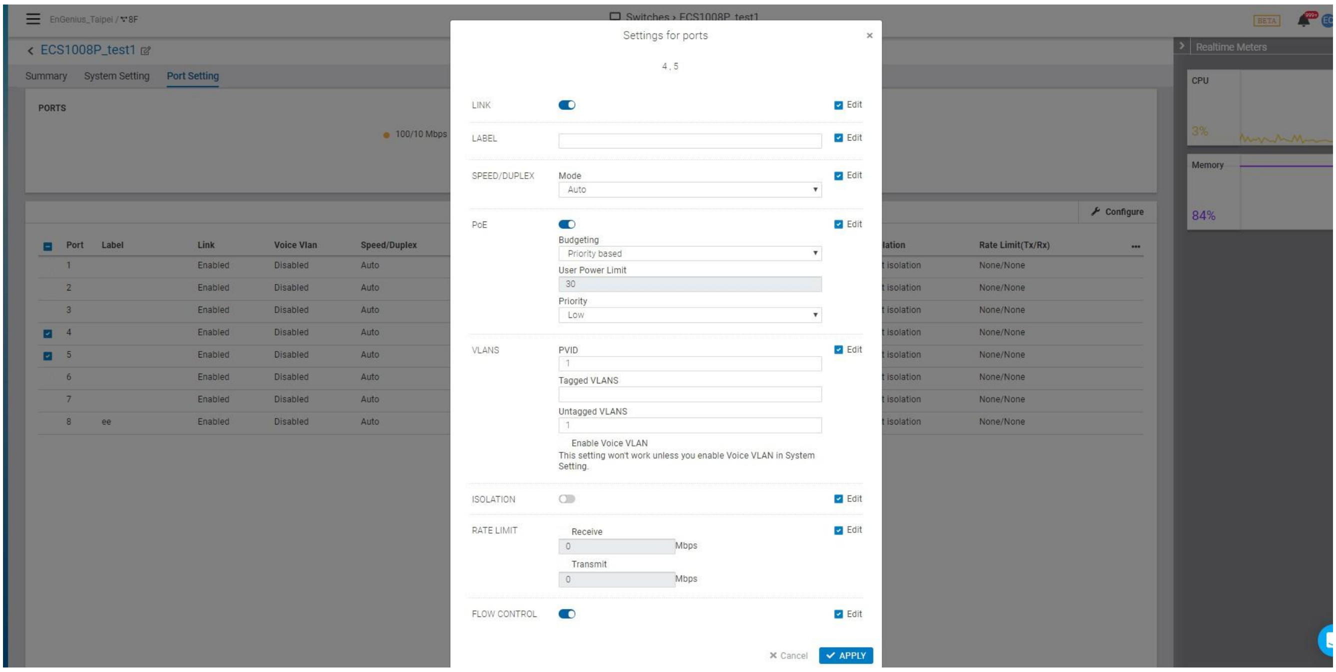
Jumbo Frames
MTU Size: 1522

## Port Settings

Selecting one or more ports and clicking **Configure** will display the following settings:



| ☐ | Port | Label | Link | Voice Vlan | Speed/Duplex | PoE | PVID | Untagged VLAN | Tagged VLAN | Isolation | Rate Limit(Tx/Rx) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 1 | | Enabled | Disabled | Auto | Low priority | 1 | 1 | - | Not isolation | None/None |
| ☐ | 2 | | Enabled | Disabled | Auto | Low priority | 1 | 1 | - | Not isolation | None/None |
| ☐ | 3 | | Enabled | Disabled | Auto | Low priority | 1 | 1 | 2 | Not isolation | None/None |
| ☑ | 4 | | Enabled | Disabled | Auto | Low priority | 1 | 1 | 2 | Not isolation | None/None |
| ☑ | 5 | | Enabled | Disabled | Auto | Low priority | 1 | 1 | - | Not isolation | None/None |
| ☐ | 6 | | Enabled | Disabled | Auto | Low priority | 1 | 1 | - | Not isolation | None/None |
| ☐ | 7 | | Enabled | Disabled | Auto | Low priority | 1 | 1 | - | Not isolation | None/None |
| ☐ | 8 | ee | Enabled | Disabled | Auto | Low priority | 1 | 1 | - | Not isolation | None/None |



Settings for ports

4 , 5

LINK ● ☑ Edit

LABEL ☑ Edit

SPEED/DUPLEX Mode: Auto ☑ Edit

PoE ● ☑ Edit
Budgeting: Priority based
User Power Limit: 30
Priority: Low

VLANS ☑ Edit
PVID: 1
Tagged VLANS:
Untagged VLANS: 1
Enable Voice VLAN
This setting won't work unless you enable Voice VLAN in System Setting.

ISOLATION ○ ☑ Edit

RATE LIMIT ☑ Edit
Receive: 0 Mbps
Transmit: 0 Mbps

FLOW CONTROL ● ☑ Edit

✕ Cancel ✓ APPLY

**Link:** Allows you to enable or disable the connection for this port.

**Label:** Allows you to add a descriptor for this port.

**Speed/Duplex:** Allows you to define the following speed/duplex communication settings for this port:

- Auto**:** Speed/Duplex will auto-negotiate based on the connected node.
- 1Gbps / Full Duplex
- 100 Mbps / Full Duplex
- 100 Mbps / Half Duplex
- 10 Mbps / Full Duplex
- 10 Mbps / Half Duplex

**Power over Ethernet (PoE):** Allows you to power a connected device through an Ethernet cable using your switch.

**VLANs:** Allows you to group devices to create a partitioned network on the same LAN.

**Isolation**: Allows you to configure a port to transmit traffic only to its connected node.

**Rate Limit**: Allows you to limit the amount of incoming and outgoing traffic in Mbps.

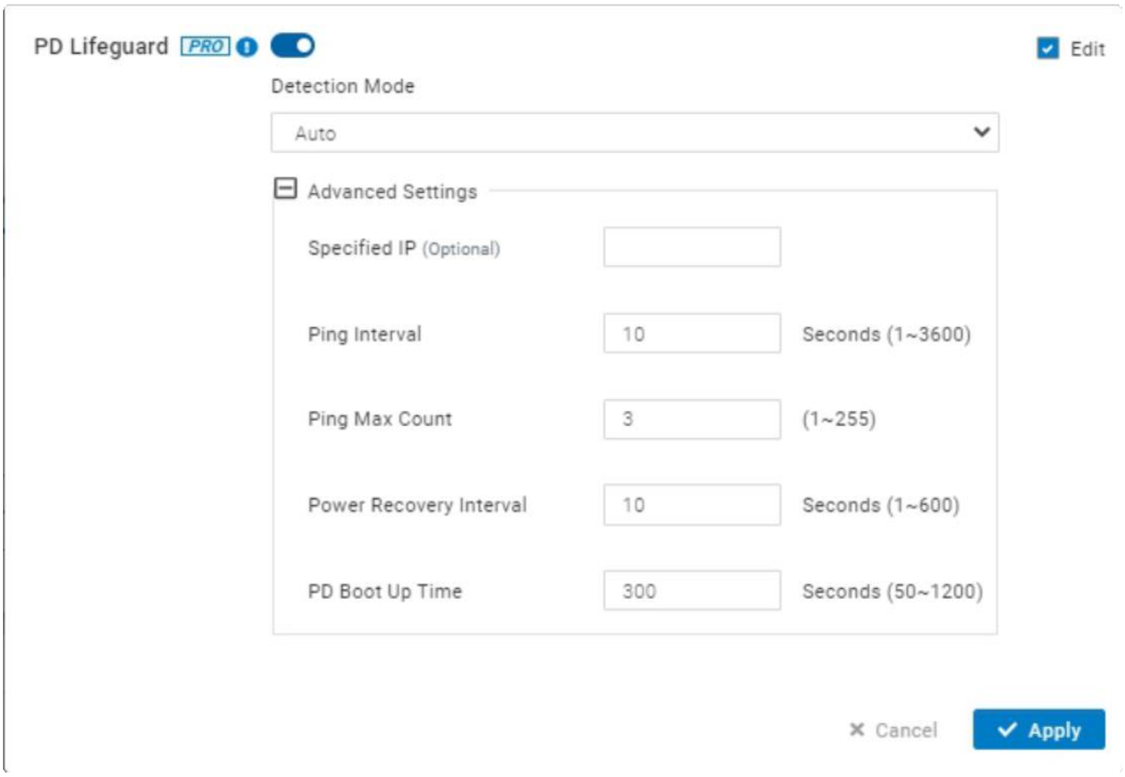
**Flow Control:** Enabling this will have the switch regulate traffic during times of congestion.

**QoS:** If QoS is enabled in **Switch Settings**, you can configure additional settings per port.

- **CoS Value:** All incoming packets that lack a CoS value will use the one set in this dropdown.
- **Trust CoS:** If checked, the switch will queue packets tagged with CoS into their designated queues. If unchecked, all packets will leave the same queue.

**PD lifeguard**: When abnormal events happen on Powered Devices, they might require reboot in order to return to normal operation. PD Lifeguard can be used to judge if the PD is still reachable and turn the unreachable devices off and on.

- **Specified IP**: Setting specified IP on a specific port.
- **Ping Interval:** Setting ping IP interval on a specific port.
- **Ping Max Count**: Setting ping max count on a specific port.
- **Power Recovery Interval:** The waiting time between power off and power on a specific port.
- **PD BootUp Time:** Setting Powered Device boot-up time on a specific port.



PD Lifeguard PRO

☑ Edit

Detection Mode: Auto

⊟ Advanced Settings

Specified IP (Optional):

Ping Interval: 10 Seconds (1~3600)

Ping Max Count: 3 (1~255)

Power Recovery Interval: 10 Seconds (1~600)

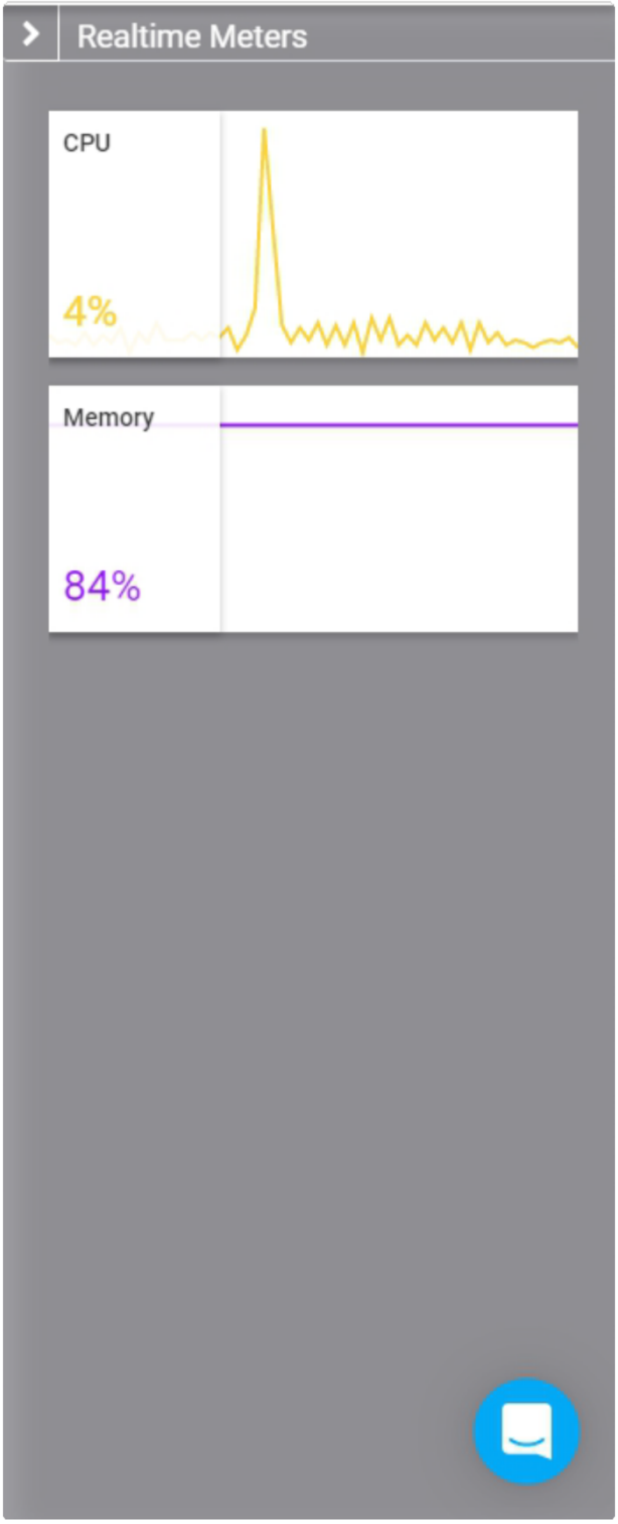
PD Boot Up Time: 300 Seconds (50~1200)

## Realtime Meters

**System Metrics** is primarily for viewing real time statistics . By default there are two types of data:

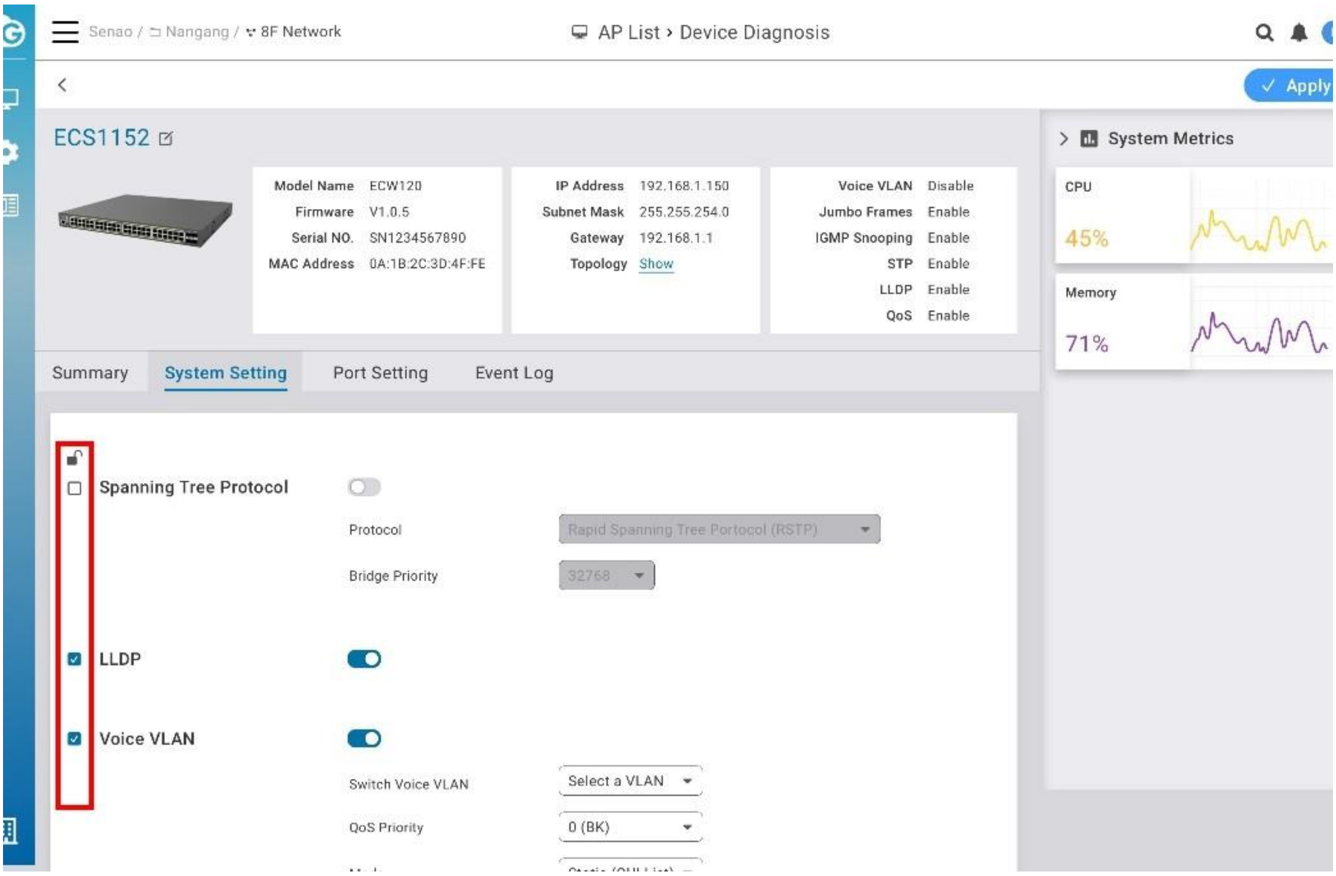
- **CPU**
- **Memory**

Capturing data over a period of time allows you to see trends useful for determining the overall performance of your switch.



## Override System setting on the Switch Network-wide setting

System setting is followed by Switch setting from the **Configure** > **Switch settings** as default settings. If you want individual AP System settings to be different from the Switch Network- wide setting , you can click below part in the screen to override the setting .



ECS1152

| | | | | | |
|---|---|---|---|---|---|
| Model Name | ECW120 | IP Address | 192.168.1.150 | Voice VLAN | Disable |
| Firmware | V1.0.5 | Subnet Mask | 255.255.254.0 | Jumbo Frames | Enable |
| Serial NO. | SN1234567890 | Gateway | 192.168.1.1 | IGMP Snooping | Enable |
| MAC Address | 0A:1B:2C:3D:4F:FE | Topology | Show | STP | Enable |
| | | | | LLDP | Enable |
| | | | | QoS | Enable |

Summary | **System Setting** | Port Setting | Event Log

☐ Spanning Tree Protocol ○

Protocol: Rapid Spanning Tree Portocol (RSTP)

Bridge Priority: 32768

☑ LLDP ●

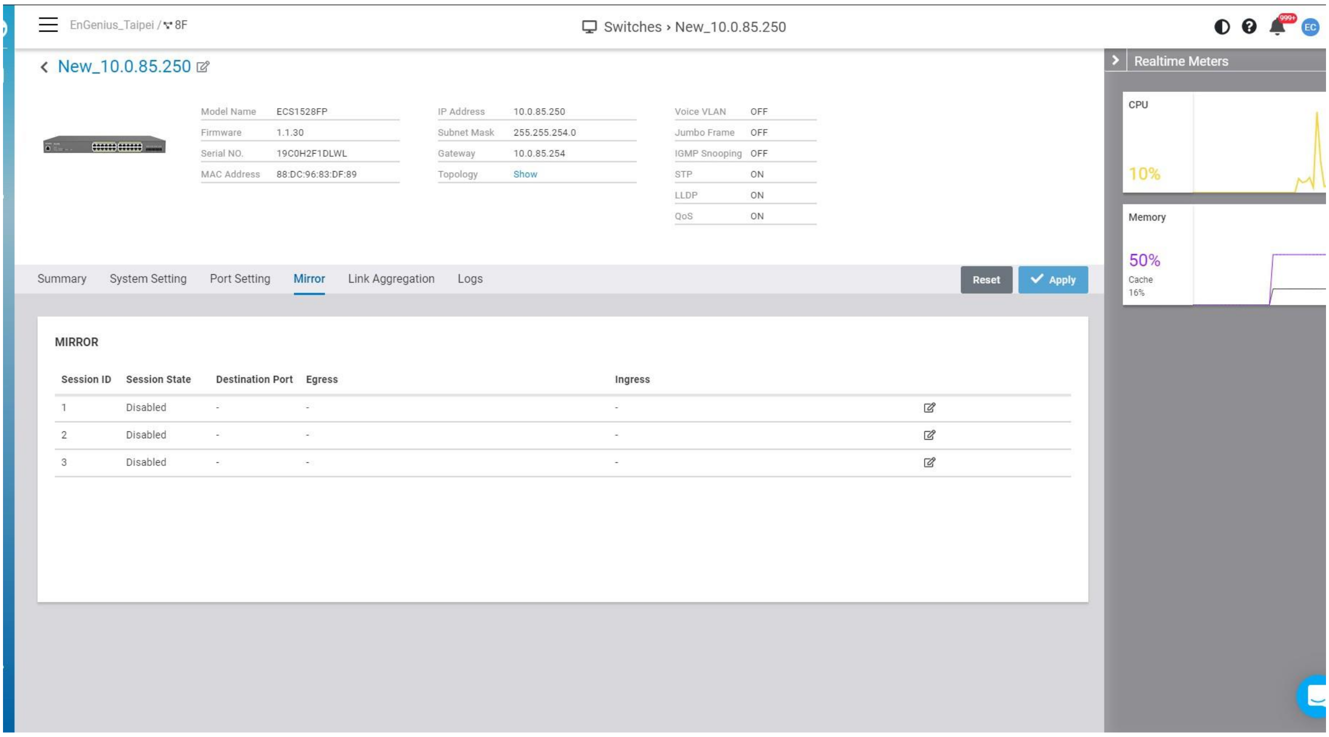
☑ Voice VLAN ●

Switch Voice VLAN: Select a VLAN

QoS Priority: 0 (BK)

## Mirror

Port Mirroring allows you to copy packets on one or more ports to a mirroring destination port. You can attach a monitoring device to the mirroring destination port to view details about the packets passing through the copied ports. This is useful for network monitoring and troubleshooting purposes. The feature is available is at **Manage** > **Switch** < **Details** > **Mirror**



New_10.0.85.250

| | | | | | |
|---|---|---|---|---|---|
| Model Name | ECS1528FP | IP Address | 10.0.85.250 | Voice VLAN | OFF |
| Firmware | 1.1.30 | Subnet Mask | 255.255.254.0 | Jumbo Frame | OFF |
| Serial NO. | 19C0H2F1DLWL | Gateway | 10.0.85.254 | IGMP Snooping | OFF |
| MAC Address | 88:DC:96:83:DF:89 | Topology | Show | STP | ON |
| | | | | LLDP | ON |
| | | | | QoS | ON |

Summary | System Setting | Port Setting | **Mirror** | Link Aggregation | Logs

MIRROR

| Session ID | Session State | Destination Port | Egress | Ingress |
|---|---|---|---|---|
| 1 | Disabled | - | - | - |
| 2 | Disabled | - | - | - |
| 3 | Disabled | - | - | - |

The following describe the labels on this screen :

**Session id** : A number identifying the mirror session. Switch supports up to 3 mirror sessions.

**Session State** : Select whether to enable or disable port mirroring.

**Destination Port :** The port which all mirrored data is sent to **.**

**Ingress** : indicates that only data being received will be mirrored.

**Egress** : indicates that only data being sent will be mirrored

## How to configure

1. Click the edit icon towards the right .
2. Enable the **Session state.**
3. Select the **Destination port**
4. Select the **Ingress** and **Egress** port
5. Click **Apply**

## Port state

There are four types of port that you configured .

| | |
|---|---|
| D | Port was assigned to a destination port . |
| E | Port was assigned only data being sent will be mirrored . |
| I | Port was assigned only data being received will be mirrored . |
| EI | Port was assigned both directions of data are being mirrored to the destination port. |

## Link Aggregation

Link aggregation groups multiple ports together in parallel to act as a single logical link. Aggregation-enabled devices treat all physical links (ports) in an aggregation group entirely as a single logical link (port). Member ports in an aggregation group share egress/ingress traffic load, delivering a bandwidth that is multiple of a single physical link. The feature is available is at **Manage** > **Switch** < **Details** > **Link**

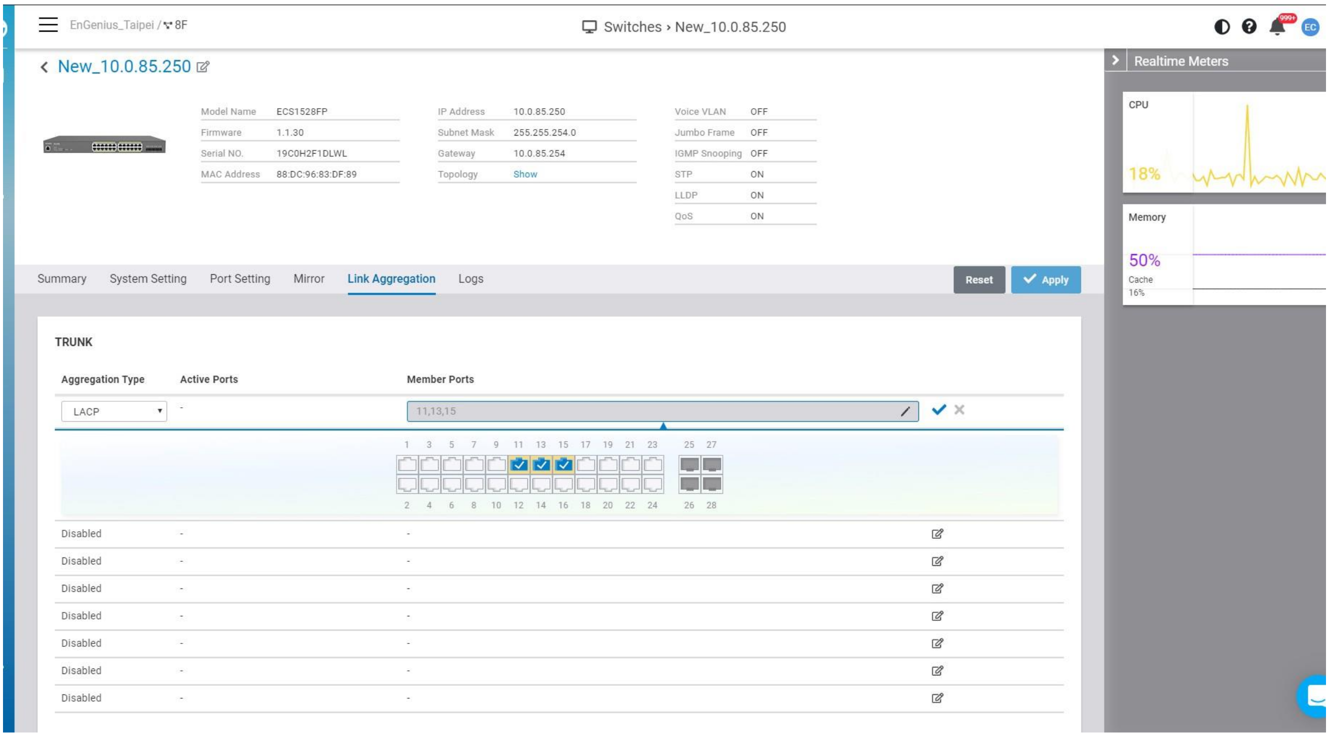
## How to Configure

To Configure trunk , you must select **aggregation type** . Select from the following options:

- **LACP**: LACP is a dynamic protocol which helps to automate the configuration and maintenance of LAG's. The main purpose of LACP is to automatically configure individual links to an aggregate bundle, while adding new links and helping to recover from link failures if the need arises. LACP can monitor to verify if all the links are connected to the authorized group. LACP is a standard in computer networking, hence LACP should be enabled on the Switch's trunk ports initially in order for both the participating Switches/devices that support the standard to use it.
- **Static:** Static configuration is used when connecting to a switch that doesn't support LACP.
- **Disable** : Disable the trunk that you configured previously.

Then select the **Member Ports** to add into the trunk group. There are two ways to select the ports

1. Click on the port picker to select multiple ports.



EnGenius_Taipei / 8F

Switches › New_10.0.85.250

New_10.0.85.250

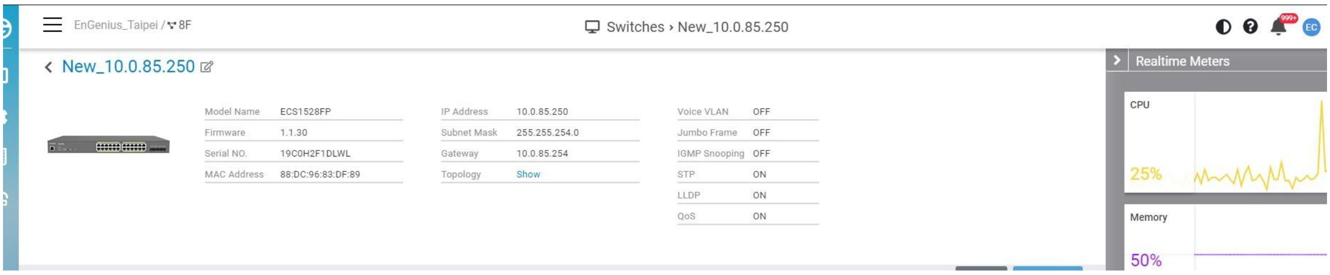
| | | | | | |
|---|---|---|---|---|---|
| Model Name | ECS1528FP | IP Address | 10.0.85.250 | Voice VLAN | OFF |
| Firmware | 1.1.30 | Subnet Mask | 255.255.254.0 | Jumbo Frame | OFF |
| Serial NO. | 19C0H2F1DLWL | Gateway | 10.0.85.254 | IGMP Snooping | OFF |
| MAC Address | 88:DC:96:83:DF:89 | Topology | Show | STP | ON |
| | | | | LLDP | ON |
| | | | | QoS | ON |

Summary | System Setting | Port Setting | Mirror | Link Aggregation | Logs

TRUNK

| Aggregation Type | Active Ports | Member Ports |
|---|---|---|
| LACP | - | 11,13,15 |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |

2. Click Pencil icon to input port numbers

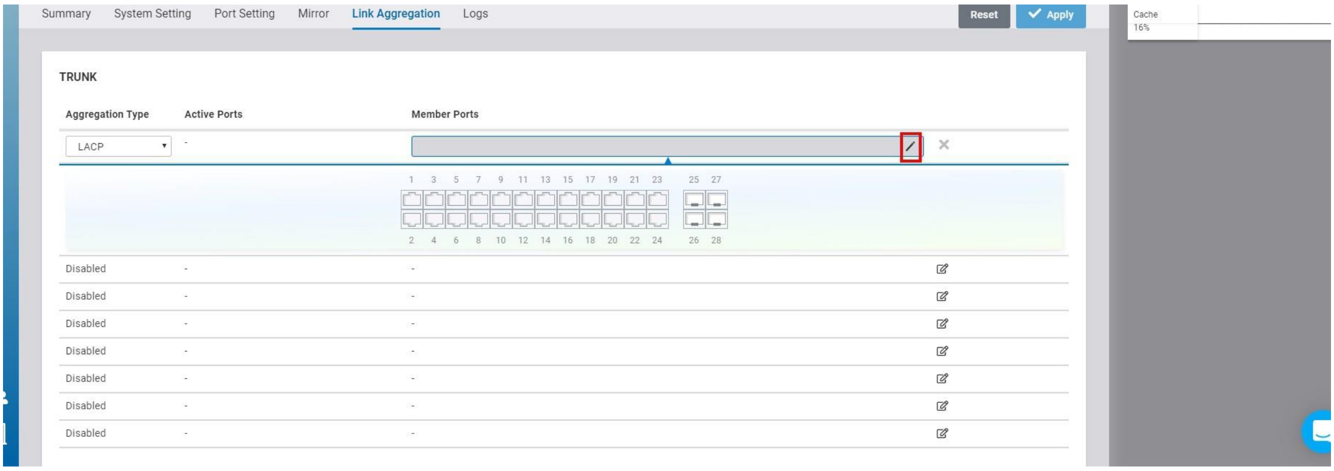


EnGenius_Taipei / 8F

Switches › New_10.0.85.250

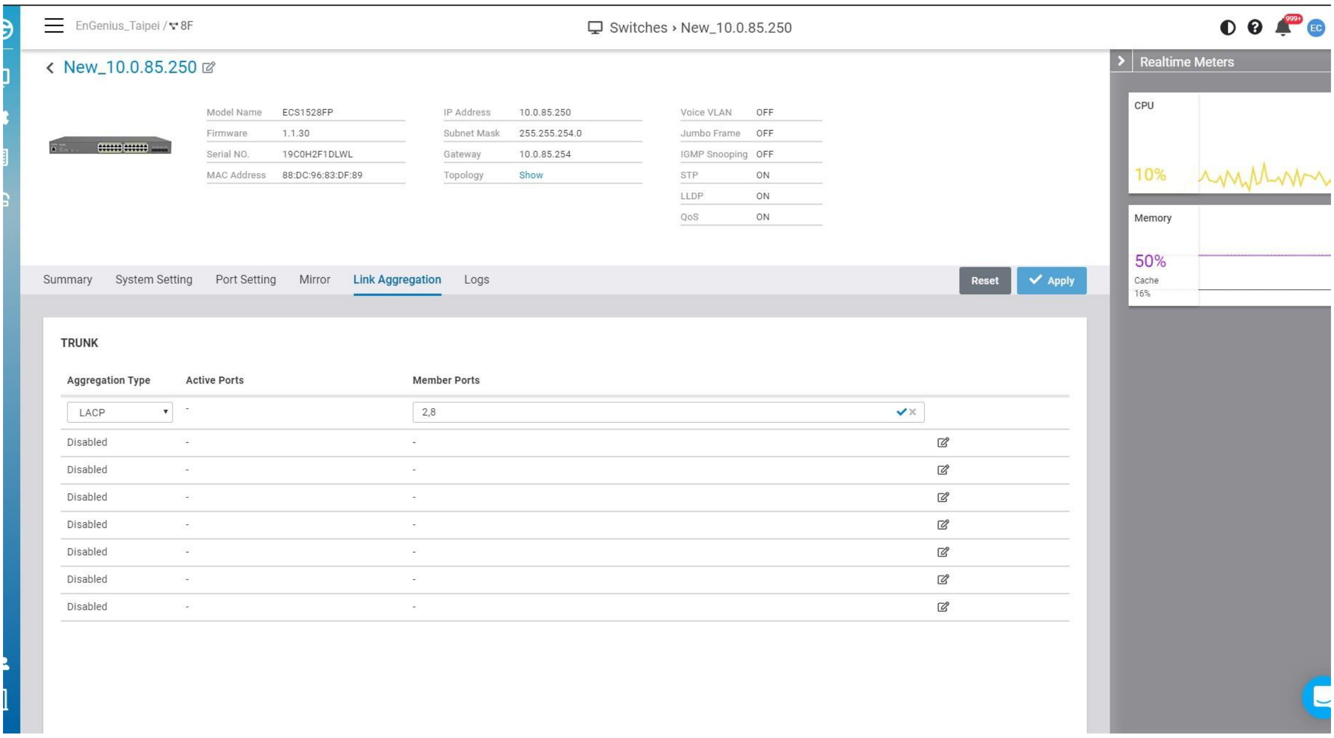
New_10.0.85.250

| | | | | | |
|---|---|---|---|---|---|
| Model Name | ECS1528FP | IP Address | 10.0.85.250 | Voice VLAN | OFF |
| Firmware | 1.1.30 | Subnet Mask | 255.255.254.0 | Jumbo Frame | OFF |
| Serial NO. | 19C0H2F1DLWL | Gateway | 10.0.85.254 | IGMP Snooping | OFF |
| MAC Address | 88:DC:96:83:DF:89 | Topology | Show | STP | ON |
| | | | | LLDP | ON |
| | | | | QoS | ON |



TRUNK

| Aggregation Type | Active Ports | Member Ports |
|---|---|---|
| LACP | - | |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |



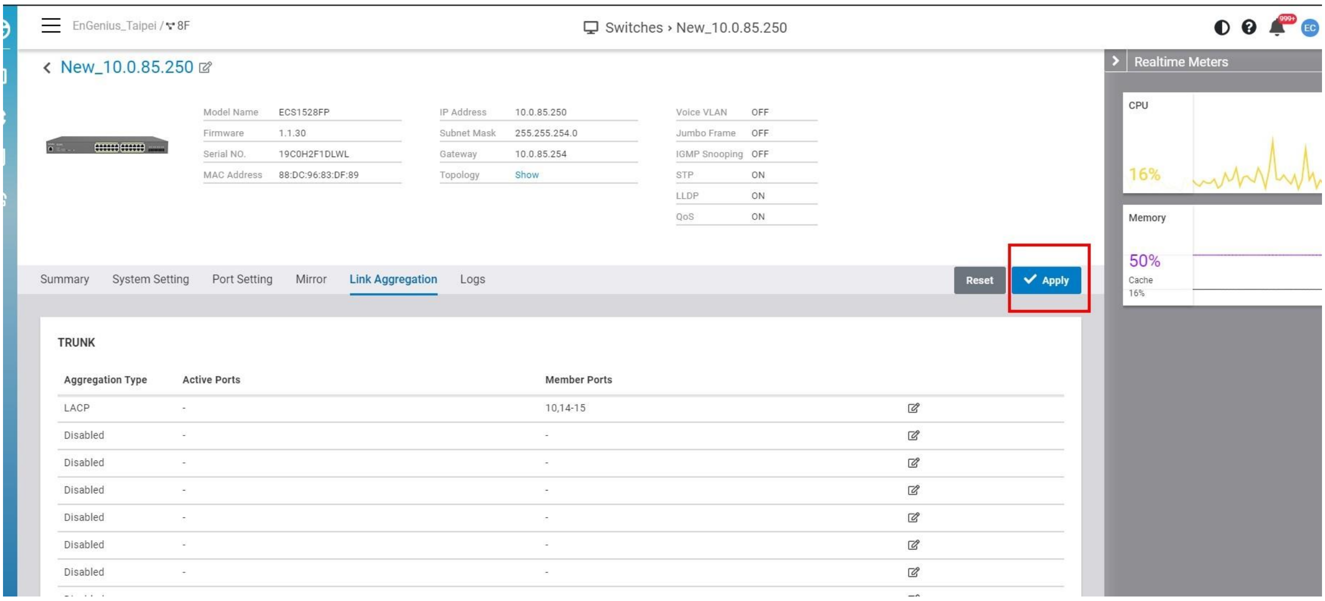
New_10.0.85.250

| | | | | | |
|---|---|---|---|---|---|
| Model Name | ECS1528FP | IP Address | 10.0.85.250 | Voice VLAN | OFF |
| Firmware | 1.1.30 | Subnet Mask | 255.255.254.0 | Jumbo Frame | OFF |
| Serial NO. | 19C0H2F1DLWL | Gateway | 10.0.85.254 | IGMP Snooping | OFF |
| MAC Address | 88:DC:96:83:DF:89 | Topology | Show | STP | ON |
| | | | | LLDP | ON |
| | | | | QoS | ON |

TRUNK

| Aggregation Type | Active Ports | Member Ports |
|---|---|---|
| LACP | - | 2,8 |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |

After you complete the trunk settings , remember to click **Apply** to take effect .

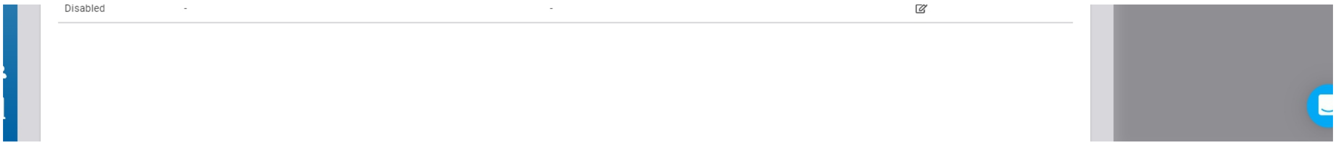


New_10.0.85.250

| | | | | | |
|---|---|---|---|---|---|
| Model Name | ECS1528FP | IP Address | 10.0.85.250 | Voice VLAN | OFF |
| Firmware | 1.1.30 | Subnet Mask | 255.255.254.0 | Jumbo Frame | OFF |
| Serial NO. | 19C0H2F1DLWL | Gateway | 10.0.85.254 | IGMP Snooping | OFF |
| MAC Address | 88:DC:96:83:DF:89 | Topology | Show | STP | ON |
| | | | | LLDP | ON |
| | | | | QoS | ON |

TRUNK

| Aggregation Type | Active Ports | Member Ports |
|---|---|---|
| LACP | - | 10,14-15 |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |
| Disabled | - | - |

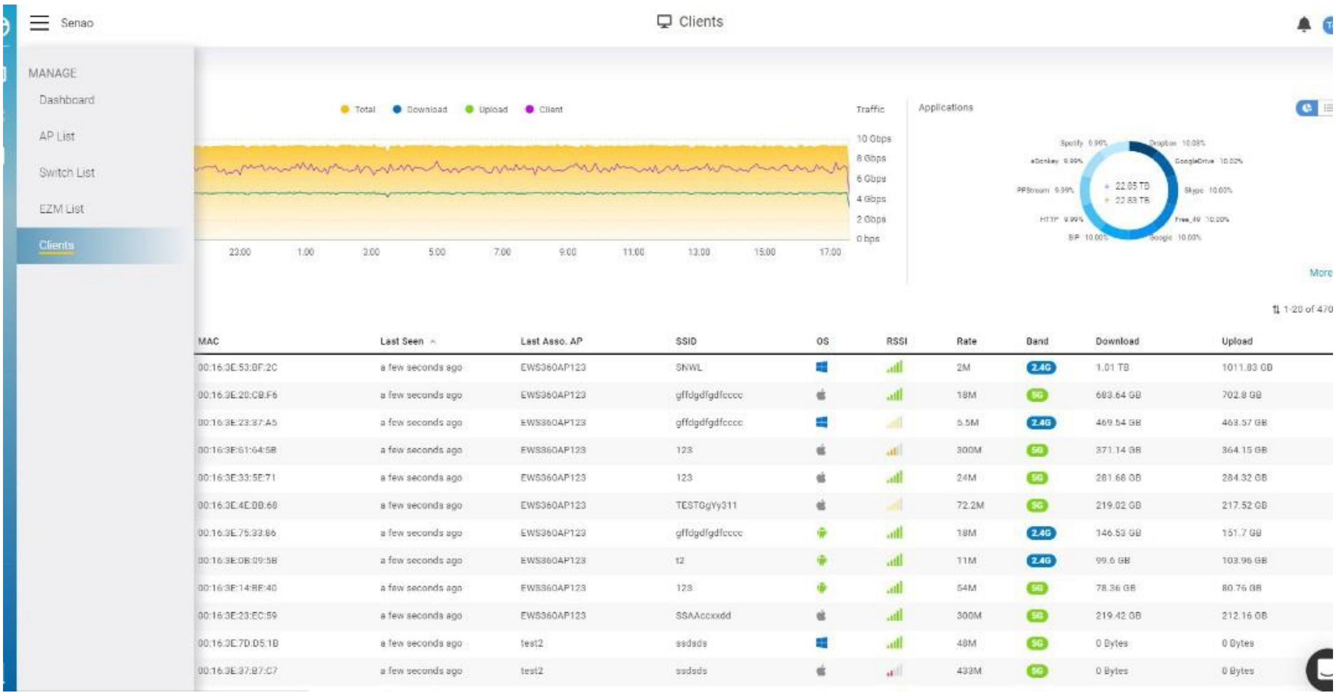


Disabled - -

# Managing Clients

EnGenius Cloud provides management views that collect information about connected clients in your organization/hierarchy view/network.

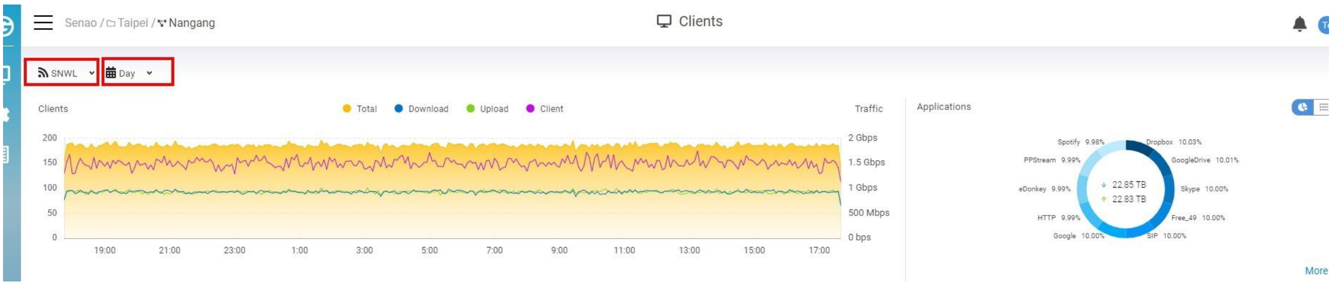
Click **Manage** -> **Clients** to access this screen and double-click the organization/hierarchy view/network on the tree to change the scope.

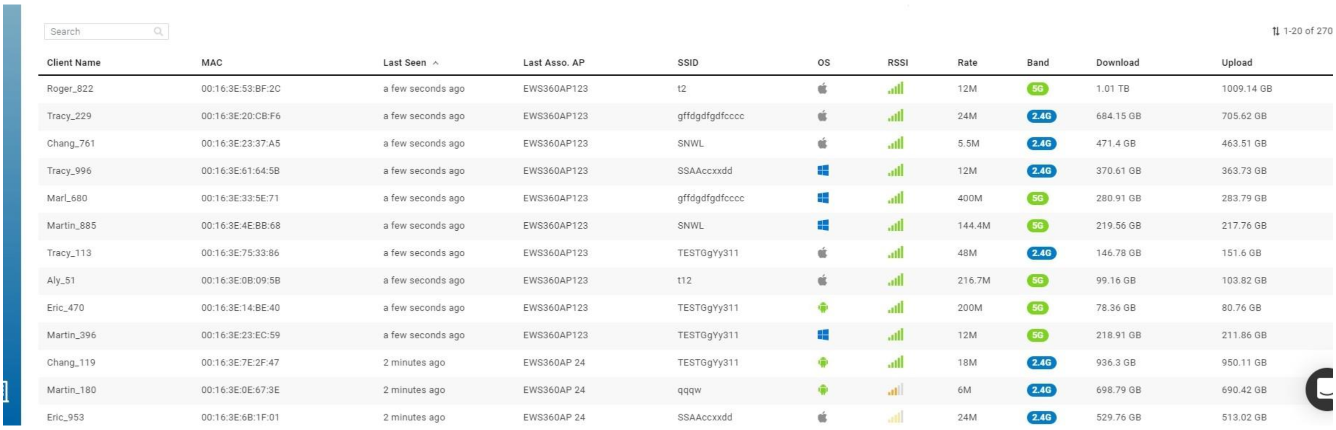


| MAC | Last Seen | Last Asso. AP | SSID | OS | RSSI | Rate | Band | Download | Upload |
|---|---|---|---|---|---|---|---|---|---|
| 00:16:3E:53:BF:2C | a few seconds ago | EWS360AP123 | SNWL | | | 2M | 2.4G | 1.01 TB | 1011.83 GB |
| 00:16:3E:20:CB:F6 | a few seconds ago | EWS360AP123 | gffdgdfgdfcccc | | | 18M | 5G | 683.64 GB | 702.8 GB |
| 00:16:3E:23:37:A5 | a few seconds ago | EWS360AP123 | gffdgdfgdfcccc | | | 5.5M | 2.4G | 469.54 GB | 463.57 GB |
| 00:16:3E:61:64:5B | a few seconds ago | EWS360AP123 | 123 | | | 300M | 5G | 371.14 GB | 364.15 GB |
| 00:16:3E:33:5E:71 | a few seconds ago | EWS360AP123 | 123 | | | 24M | 5G | 281.68 GB | 284.32 GB |
| 00:16:3E:4E:DB:68 | a few seconds ago | EWS360AP123 | TESTGgYy311 | | | 72.2M | 5G | 219.02 GB | 217.52 GB |
| 00:16:3E:75:33:86 | a few seconds ago | EWS360AP123 | gffdgdfgdfcccc | | | 18M | 2.4G | 146.53 GB | 151.7 GB |
| 00:16:3E:0B:09:5B | a few seconds ago | EWS360AP123 | t2 | | | 11M | 2.4G | 99.6 GB | 103.96 GB |
| 00:16:3E:14:BE:40 | a few seconds ago | EWS360AP123 | 123 | | | 54M | 5G | 78.36 GB | 80.76 GB |
| 00:16:3E:23:EC:59 | a few seconds ago | EWS360AP123 | SSAAccxxdd | | | 300M | 5G | 219.42 GB | 212.16 GB |
| 00:16:3E:7D:D5:1B | a few seconds ago | test2 | ssdsds | | | 48M | 5G | 0 Bytes | 0 Bytes |
| 00:16:3E:37:B7:C7 | a few seconds ago | test2 | ssdsds | | | 433M | 5G | 0 Bytes | 0 Bytes |

# Filtering the Clients List

The list of clients can be customized based on time intervals, and the chart can be customized based on time intervals and SSIDs. To change these parameters, use the appropriate dropdown menu at the top of the screen.





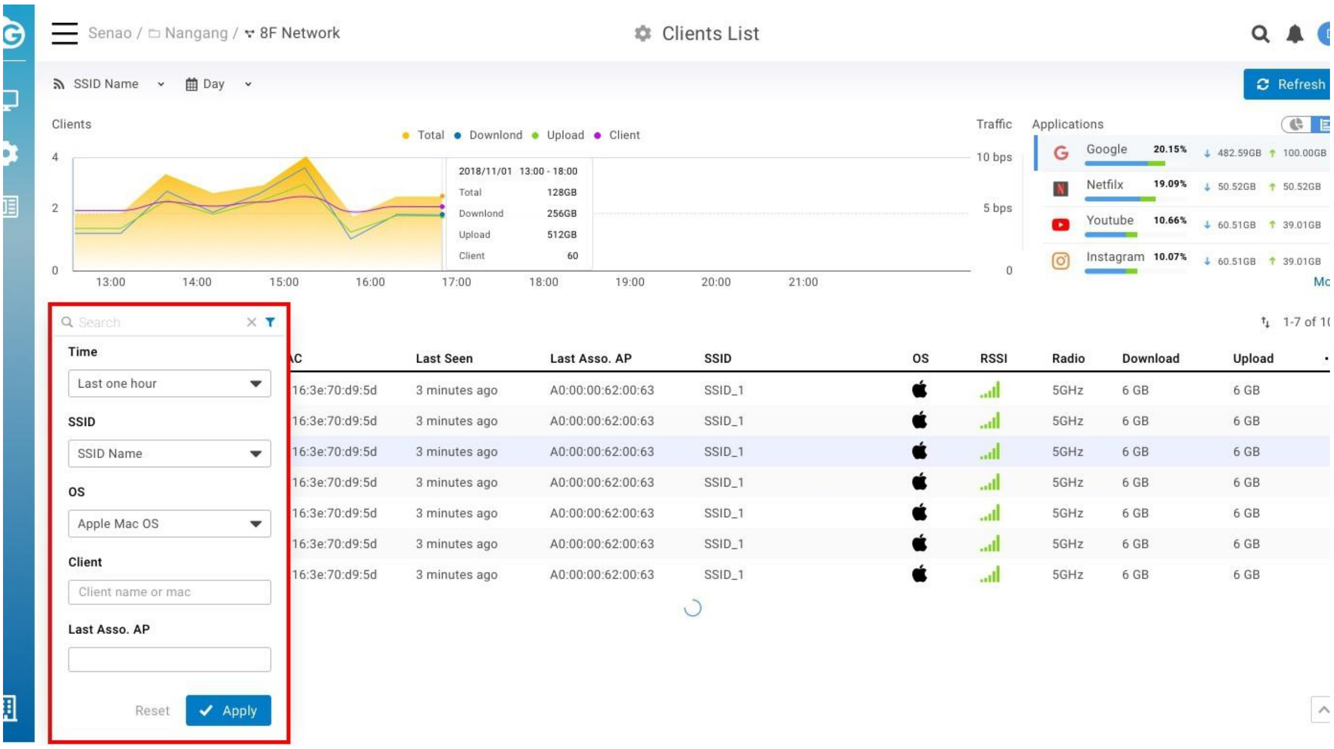
Search

1-20 of 270

| Client Name | MAC | Last Seen | Last Asso. AP | SSID | OS | RSSI | Rate | Band | Download | Upload |
|---|---|---|---|---|---|---|---|---|---|---|
| Roger_822 | 00:16:3E:53:BF:2C | a few seconds ago | EWS360AP123 | t2 |  |  | 12M | 5G | 1.01 TB | 1009.14 GB |
| Tracy_229 | 00:16:3E:20:CB:F6 | a few seconds ago | EWS360AP123 | gffdgdfgdfcccc |  |  | 24M | 2.4G | 684.15 GB | 705.62 GB |
| Chang_761 | 00:16:3E:23:37:A5 | a few seconds ago | EWS360AP123 | SNWL |  |  | 5.5M | 2.4G | 471.4 GB | 463.51 GB |
| Tracy_996 | 00:16:3E:61:64:5B | a few seconds ago | EWS360AP123 | SSAAccxxdd |  |  | 12M | 2.4G | 370.61 GB | 363.73 GB |
| Marl_680 | 00:16:3E:33:5E:71 | a few seconds ago | EWS360AP123 | gffdgdfgdfcccc |  |  | 400M | 5G | 280.91 GB | 283.79 GB |
| Martin_885 | 00:16:3E:4E:BB:68 | a few seconds ago | EWS360AP123 | SNWL |  |  | 144.4M | 5G | 219.56 GB | 217.76 GB |
| Tracy_113 | 00:16:3E:75:33:86 | a few seconds ago | EWS360AP123 | TESTGgYy311 |  |  | 48M | 2.4G | 146.78 GB | 151.6 GB |
| Aly_51 | 00:16:3E:0B:09:5B | a few seconds ago | EWS360AP123 | t12 |  |  | 216.7M | 5G | 99.16 GB | 103.82 GB |
| Eric_470 | 00:16:3E:14:BE:40 | a few seconds ago | EWS360AP123 | TESTGgYy311 |  |  | 200M | 5G | 78.36 GB | 80.76 GB |
| Martin_396 | 00:16:3E:23:EC:59 | a few seconds ago | EWS360AP123 | TESTGgYy311 |  |  | 12M | 5G | 218.91 GB | 211.86 GB |
| Chang_119 | 00:16:3E:7E:2F:47 | 2 minutes ago | EWS360AP 24 | TESTGgYy311 |  |  | 18M | 2.4G | 936.3 GB | 950.11 GB |
| Martin_180 | 00:16:3E:0E:67:3E | 2 minutes ago | EWS360AP 24 | qqqw |  |  | 6M | 2.4G | 698.79 GB | 690.42 GB |
| Eric_953 | 00:16:3E:6B:1F:01 | 2 minutes ago | EWS360AP 24 | SSAAccxxdd |  |  | 24M | 2.4G | 529.76 GB | 513.02 GB |

## Searching for Clients

You can search for a client in the current client list by using the search. You can search by any parameter included in the search options, and it will attempt to match your query across all fields. You can also specify multiple parameters by clicking on the icon in the search box, as seen below:



Search

Time: Last one hour

SSID: SSID Name

OS: Apple Mac OS

Client: Client name or mac

Last Asso. AP:

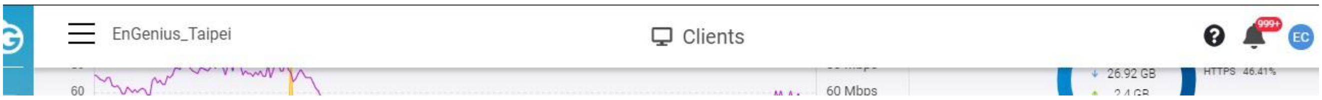
Reset ✓ Apply

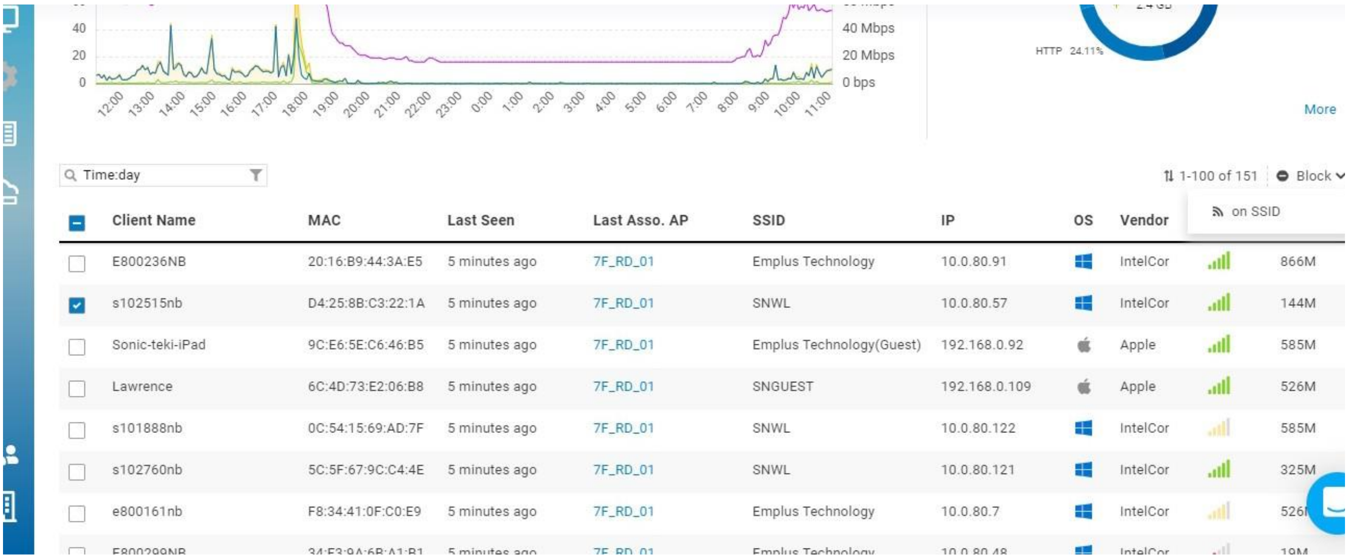
1-7 of 1(

| AC | Last Seen | Last Asso. AP | SSID | OS | RSSI | Radio | Download | Upload |
|---|---|---|---|---|---|---|---|---|
| 16:3e:70:d9:5d | 3 minutes ago | A0:00:00:62:00:63 | SSID_1 |  |  | 5GHz | 6 GB | 6 GB |
| 16:3e:70:d9:5d | 3 minutes ago | A0:00:00:62:00:63 | SSID_1 |  |  | 5GHz | 6 GB | 6 GB |
| 16:3e:70:d9:5d | 3 minutes ago | A0:00:00:62:00:63 | SSID_1 |  |  | 5GHz | 6 GB | 6 GB |
| 16:3e:70:d9:5d | 3 minutes ago | A0:00:00:62:00:63 | SSID_1 |  |  | 5GHz | 6 GB | 6 GB |
| 16:3e:70:d9:5d | 3 minutes ago | A0:00:00:62:00:63 | SSID_1 |  |  | 5GHz | 6 GB | 6 GB |
| 16:3e:70:d9:5d | 3 minutes ago | A0:00:00:62:00:63 | SSID_1 |  |  | 5GHz | 6 GB | 6 GB |
| 16:3e:70:d9:5d | 3 minutes ago | A0:00:00:62:00:63 | SSID_1 |  |  | 5GHz | 6 GB | 6 GB |

## Block Clients

This allows you to block clients on the current SSID that clients connected .



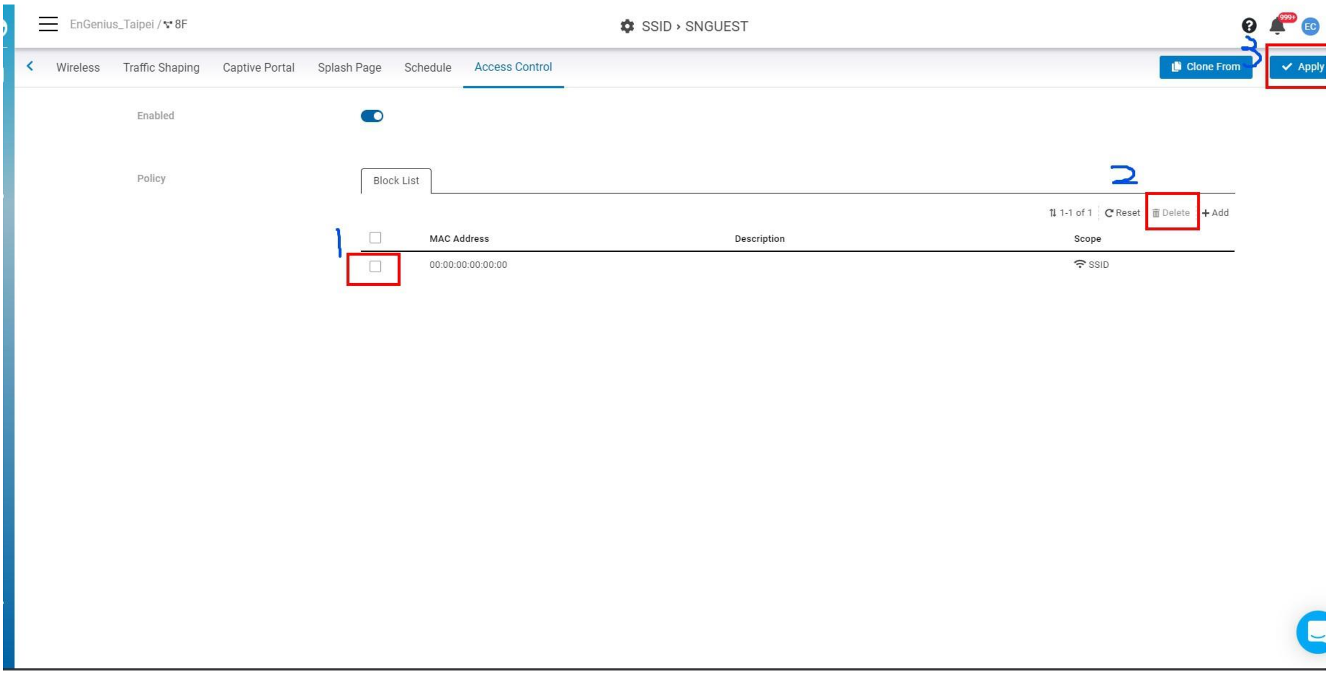


Time:day

1-100 of 151 Block on SSID

| | Client Name | MAC | Last Seen | Last Asso. AP | SSID | IP | OS | Vendor | | |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | E800236NB | 20:16:B9:44:3A:E5 | 5 minutes ago | 7F_RD_01 | Emplus Technology | 10.0.80.91 | | IntelCor | | 866M |
| ☑ | s102515nb | D4:25:8B:C3:22:1A | 5 minutes ago | 7F_RD_01 | SNWL | 10.0.80.57 | | IntelCor | | 144M |
| □ | Sonic-teki-iPad | 9C:E6:5E:C6:46:B5 | 5 minutes ago | 7F_RD_01 | Emplus Technology(Guest) | 192.168.0.92 | | Apple | | 585M |
| □ | Lawrence | 6C:4D:73:E2:06:B8 | 5 minutes ago | 7F_RD_01 | SNGUEST | 192.168.0.109 | | Apple | | 526M |
| □ | s101888nb | 0C:54:15:69:AD:7F | 5 minutes ago | 7F_RD_01 | SNWL | 10.0.80.122 | | IntelCor | | 585M |
| □ | s102760nb | 5C:5F:67:9C:C4:4E | 5 minutes ago | 7F_RD_01 | SNWL | 10.0.80.121 | | IntelCor | | 325M |
| □ | e800161nb | F8:34:41:0F:C0:E9 | 5 minutes ago | 7F_RD_01 | Emplus Technology | 10.0.80.7 | | IntelCor | | 526M |
| □ | E800299NB | 34:F3:9A:6B:A1:B1 | 5 minutes ago | 7F_RD_01 | Emplus Technology | 10.0.80.48 | | IntelCor | | 19M |

Once you want to unblock clients , please go to **Configure** > **SSID** > **Access control** to delete the Mac Address from the Block list .



Enabled ●

Policy

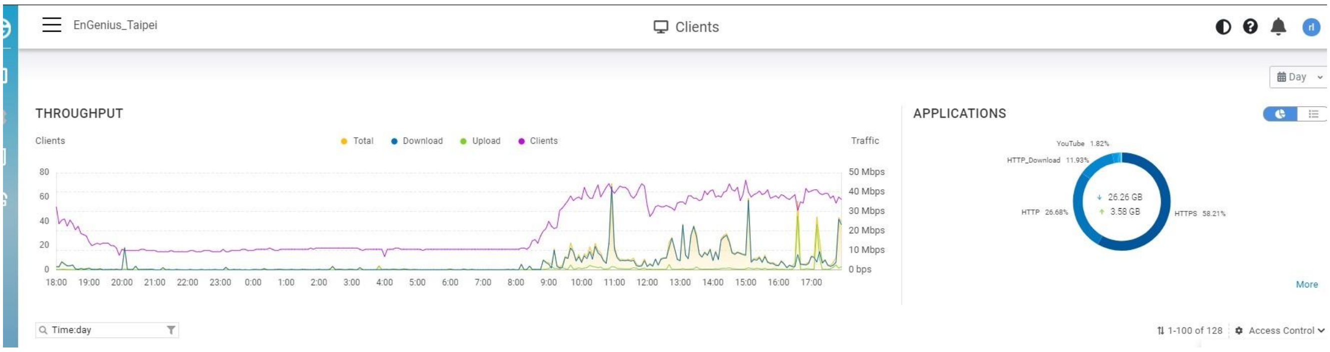
Block List

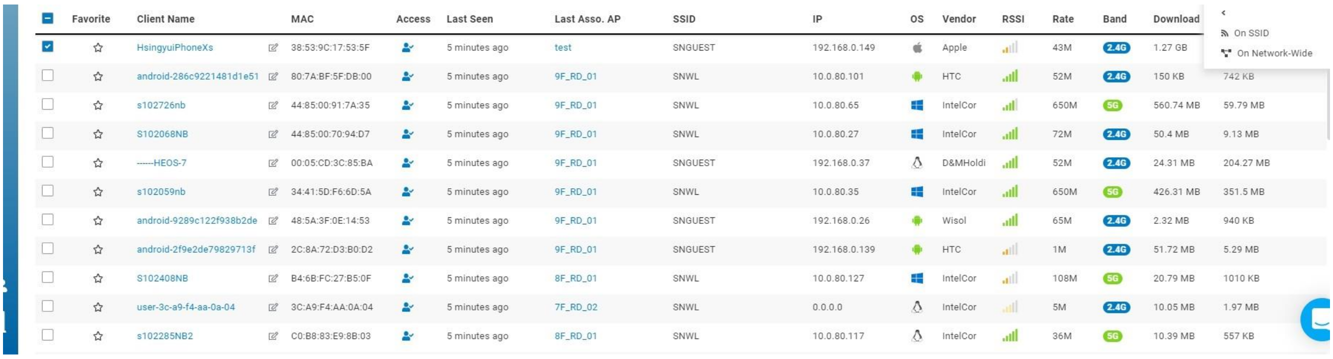
1-1 of 1 Reset Delete + Add

| □ | MAC Address | Description | Scope |
|---|---|---|---|
| □ | 00:00:00:00:00:00 | | SSID |

## VIP Clients

This allows you to make clients as VIP on the current SSID or on Network-wide that clients connected.



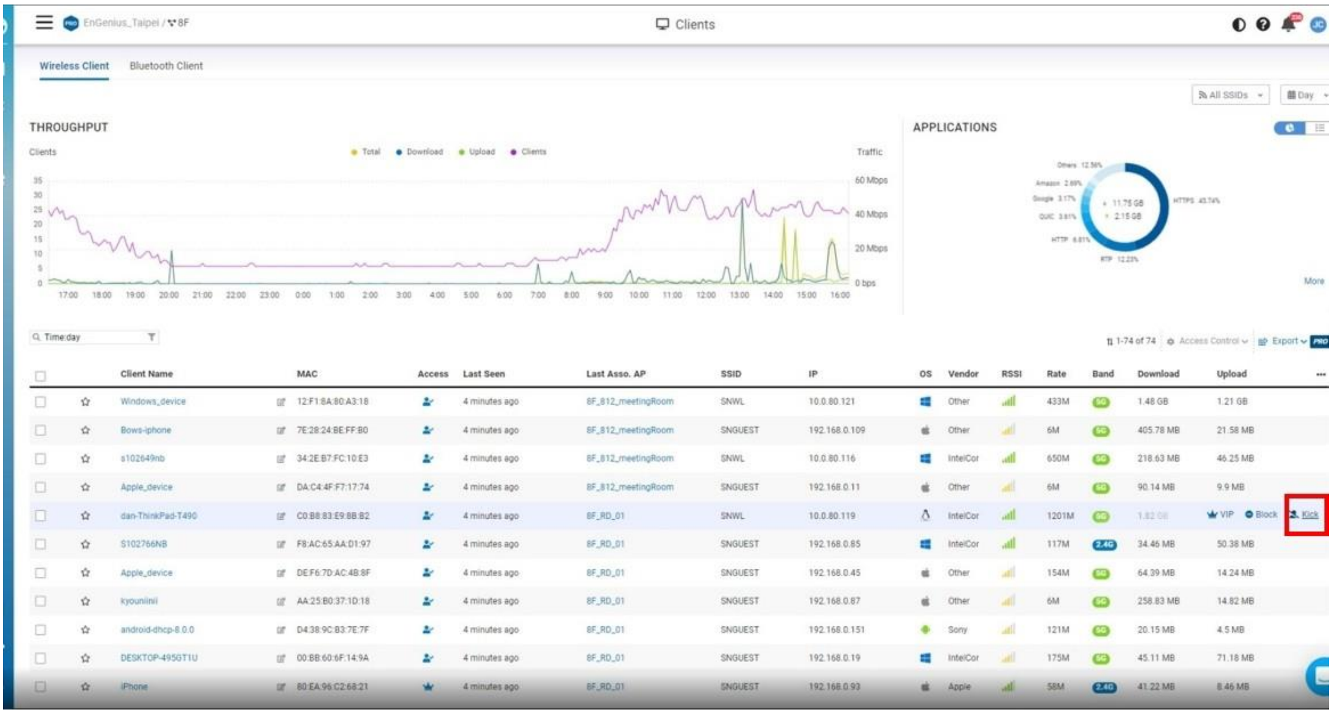


| | Favorite | Client Name | MAC | Access | Last Seen | Last Asso. AP | SSID | IP | OS | Vendor | RSSI | Rate | Band | Download | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | ☆ | HsingyuiPhoneXs | 38:53:9C:17:53:5F | | 5 minutes ago | test | SNGUEST | 192.168.0.149 | | Apple | | 43M | 2.4G | 1.27 GB | |
| □ | ☆ | android-286c9221481d1e51 | 80:7A:BF:5F:DB:00 | | 5 minutes ago | 9F_RD_01 | SNWL | 10.0.80.101 | | HTC | | 52M | 2.4G | 150 KB | 742 KB |
| □ | ☆ | s102726nb | 44:85:00:91:7A:35 | | 5 minutes ago | 9F_RD_01 | SNWL | 10.0.80.65 | | IntelCor | | 650M | 5G | 560.74 MB | 59.79 MB |
| □ | ☆ | S102068NB | 44:85:00:70:94:D7 | | 5 minutes ago | 9F_RD_01 | SNWL | 10.0.80.27 | | IntelCor | | 72M | 2.4G | 50.4 MB | 9.13 MB |
| □ | ☆ | ------HEOS-7 | 00:05:CD:3C:85:BA | | 5 minutes ago | 9F_RD_01 | SNGUEST | 192.168.0.37 | | D&MHoldi | | 52M | 2.4G | 24.31 MB | 204.27 MB |
| □ | ☆ | s102059nb | 34:41:5D:F6:6D:5A | | 5 minutes ago | 9F_RD_01 | SNWL | 10.0.80.35 | | IntelCor | | 650M | 5G | 426.31 MB | 351.5 MB |
| □ | ☆ | android-9289c122f938b2de | 48:5A:3F:0E:14:53 | | 5 minutes ago | 9F_RD_01 | SNGUEST | 192.168.0.26 | | Wisol | | 65M | 2.4G | 2.32 MB | 940 KB |
| □ | ☆ | android-2f9e2de79829713f | 2C:8A:72:D3:B0:D2 | | 5 minutes ago | 9F_RD_01 | SNGUEST | 192.168.0.139 | | HTC | | 1M | 2.4G | 51.72 MB | 5.29 MB |
| □ | ☆ | S102408NB | B4:6B:FC:27:B5:0F | | 5 minutes ago | 8F_RD_01 | SNWL | 10.0.80.127 | | IntelCor | | 108M | 5G | 20.79 MB | 1010 KB |
| □ | ☆ | user-3c-a9-f4-aa-0a-04 | 3C:A9:F4:AA:0A:04 | | 5 minutes ago | 7F_RD_02 | SNWL | 0.0.0.0 | | IntelCor | | 5M | 2.4G | 10.05 MB | 1.97 MB |
| □ | ☆ | s102285NB2 | C0:B8:83:E9:8B:03 | | 5 minutes ago | 8F_RD_01 | SNWL | 10.0.80.117 | | IntelCor | | 36M | 5G | 10.39 MB | 557 KB |

Once you want to delete clients from the VIP list, please go to **Configure** > **Access control** to delete the Mac Address from the VIP list.

## Kick Clients

If you don't want to block clients permanently, you could just kick them so that they can connect again if they want to.



| □ | | Client Name | MAC | Access | Last Seen | Last Asso. AP | SSID | IP | OS | Vendor | RSSI | Rate | Band | Download | Upload |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | ☆ | Windows_device | 12:F1:8A:80:A3:18 | | 4 minutes ago | 8F_812_meetingRoom | SNWL | 10.0.80.121 | | Other | | 433M | 5G | 1.48 GB | 1.21 GB |
| □ | ☆ | Bows-iphone | 7E:28:24:BE:FF:B0 | | 4 minutes ago | 8F_812_meetingRoom | SNGUEST | 192.168.0.109 | | Other | | 6M | 5G | 405.78 MB | 21.58 MB |
| □ | ☆ | s102649nb | 34:2E:B7:FC:10:E3 | | 4 minutes ago | 8F_812_meetingRoom | SNWL | 10.0.80.116 | | IntelCor | | 650M | 5G | 218.63 MB | 46.25 MB |
| □ | ☆ | Apple_device | DA:C4:4F:F7:17:74 | | 4 minutes ago | 8F_812_meetingRoom | SNGUEST | 192.168.0.11 | | Other | | 6M | 5G | 90.14 MB | 9.9 MB |
| □ | ☆ | dan-ThinkPad-T490 | C0:B8:83:E9:8B:B2 | | 4 minutes ago | 8F_RD_01 | SNWL | 10.0.80.119 | | IntelCor | | 1201M | 5G | 1.82 GB | VIP Block Kick |
| □ | ☆ | S102766NB | F8:AC:65:AA:D1:97 | | 4 minutes ago | 8F_RD_01 | SNGUEST | 192.168.0.85 | | IntelCor | | 117M | 2.4G | 34.46 MB | 50.38 MB |
| □ | ☆ | Apple_device | DE:F6:7D:AC:4B:8F | | 4 minutes ago | 8F_RD_01 | SNGUEST | 192.168.0.45 | | Other | | 154M | 5G | 64.39 MB | 14.24 MB |
| □ | ☆ | kyouniinii | AA:25:B0:37:1D:18 | | 4 minutes ago | 8F_RD_01 | SNGUEST | 192.168.0.87 | | Other | | 6M | 5G | 258.83 MB | 14.82 MB |
| □ | ☆ | android-dhcp-8.0.0 | D4:38:9C:B3:7E:7F | | 4 minutes ago | 8F_RD_01 | SNGUEST | 192.168.0.151 | | Sony | | 121M | 5G | 20.15 MB | 4.5 MB |
| □ | ☆ | DESKTOP-495GT1U | 00:BB:60:6F:14:9A | | 4 minutes ago | 8F_RD_01 | SNGUEST | 192.168.0.19 | | IntelCor | | 175M | 5G | 45.11 MB | 71.18 MB |
| □ | ☆ | iPhone | 80:EA:96:C2:68:21 | | 4 minutes ago | 8F_RD_01 | SNGUEST | 192.168.0.93 | | Apple | | 58M | 2.4G | 41.22 MB | 8.46 MB |

## Client Timeline

The Client Timeline is a great feature that aggregates and analyzes activities of a specific wireless client to provide an intuitive and historical view. With Client Timeline, user can easily know how clients associate, authenticate, and roam among Access Points. It is extremely useful when you need to debug or trace your wireless network. The feature is available at **Manage** > **Client** > **Client name**.

# Client States

The EnGenius Cloud AI system categorizes client activities into five different states:

Client was connecting to an AP.

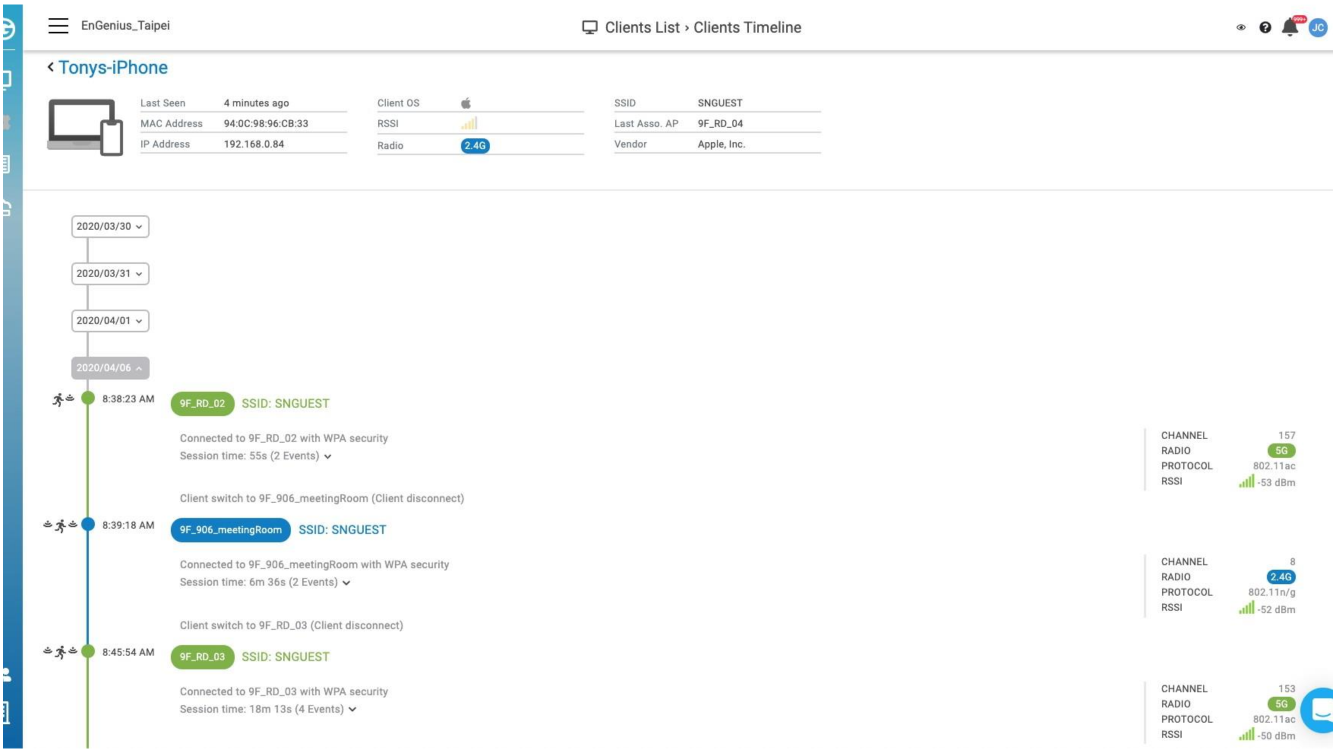
Client was roaming and connecting to another AP.

Client changed to associate with different radio or SSID of the same AP.

Client failed to authenticate with an SSID.

Client was denied because of it is in block list.

The states are displayed at the left hand side of timeline. User can easily see how a client transited its states among APs.



‹ Tonys-iPhone

| | | | | | |
|---|---|---|---|---|---|
| Last Seen | 4 minutes ago | Client OS | | SSID | SNGUEST |
| MAC Address | 94:0C:98:96:CB:33 | RSSI | | Last Asso. AP | 9F_RD_04 |
| IP Address | 192.168.0.84 | Radio | 2.4G | Vendor | Apple, Inc. |

2020/03/30
2020/03/31
2020/04/01
2020/04/06

8:38:23 AM 9F_RD_02 SSID: SNGUEST

Connected to 9F_RD_02 with WPA security
Session time: 55s (2 Events)

| | |
|---|---|
| CHANNEL | 157 |
| RADIO | 5G |
| PROTOCOL | 802.11ac |
| RSSI | -53 dBm |

Client switch to 9F_906_meetingRoom (Client disconnect)

8:39:18 AM 9F_906_meetingRoom SSID: SNGUEST

Connected to 9F_906_meetingRoom with WPA security
Session time: 6m 36s (2 Events)

| | |
|---|---|
| CHANNEL | 8 |
| RADIO | 2.4G |
| PROTOCOL | 802.11n/g |
| RSSI | -52 dBm |

Client switch to 9F_RD_03 (Client disconnect)

8:45:54 AM 9F_RD_03 SSID: SNGUEST

Connected to 9F_RD_03 with WPA security
Session time: 18m 13s (4 Events)

| | |
|---|---|
| CHANNEL | 153 |
| RADIO | 5G |
| PROTOCOL | 802.11ac |
| RSSI | -50 dBm |

# Radio Color Conventions

The drawing and content of client timeline follows the color conventions as below:

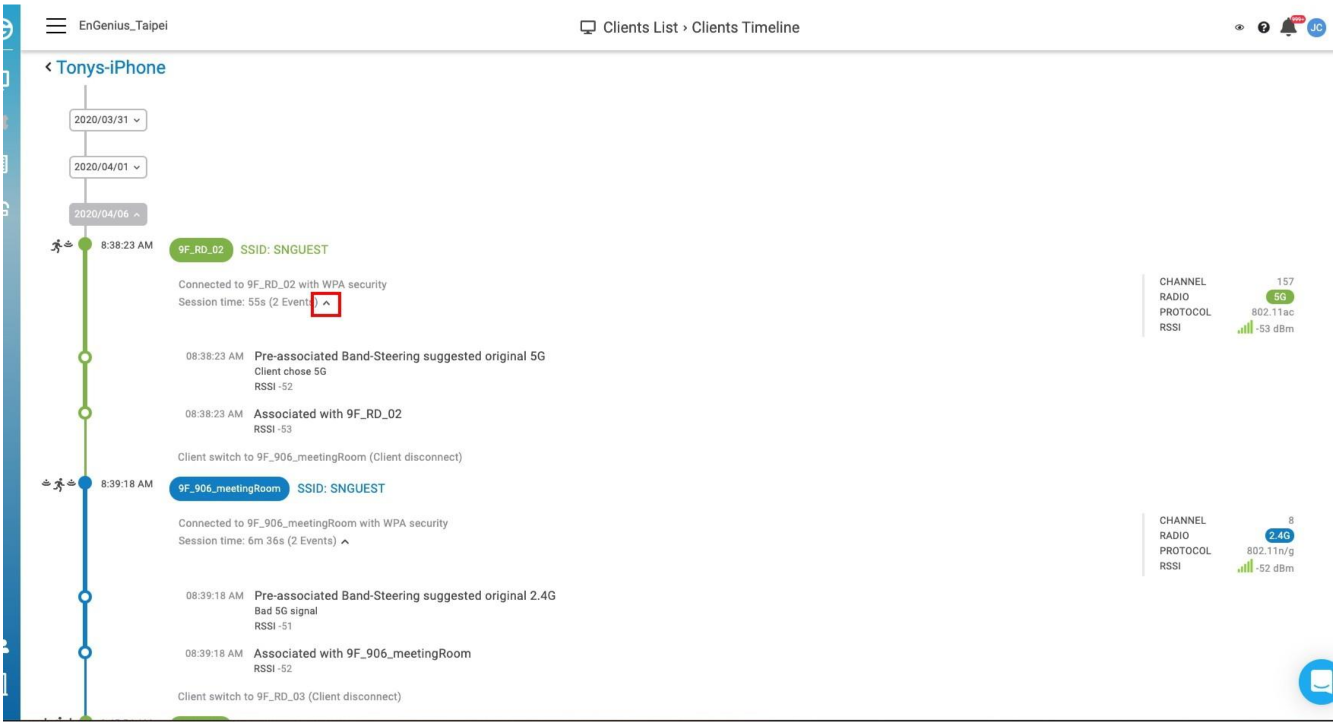
- Green: represent a 5G session.
- Blue: represent a 2.4G session.

> In the right hand side of each session, the system shows the channel, band, protocol, and signal strength of client detected at the beginning of that session.

## Transition Details

The communication between wireless client and AP could be very complicated. Different clients with different wifi chips and wireless drivers can behave very differently while communicating with the same AP. The intelligent engine behind Client Timeline is capable of analyzing communication packets effectively and performs clean and human readable transition details for the user.

User can click on the event summary inside a connection session to expand the sequence of transition details:



8:38:23 AM 9F_RD_02 SSID: SNGUEST

Connected to 9F_RD_02 with WPA security
Session time: 55s (2 Events)

CHANNEL 157
RADIO 5G
PROTOCOL 802.11ac
RSSI -53 dBm

08:38:23 AM Pre-associated Band-Steering suggested original 5G
Client chose 5G
RSSI -52

08:38:23 AM Associated with 9F_RD_02
RSSI -53

Client switch to 9F_906_meetingRoom (Client disconnect)

8:39:18 AM 9F_906_meetingRoom SSID: SNGUEST

Connected to 9F_906_meetingRoom with WPA security
Session time: 6m 36s (2 Events)

CHANNEL 8
RADIO 2.4G
PROTOCOL 802.11n/g
RSSI -52 dBm

08:39:18 AM Pre-associated Band-Steering suggested original 2.4G
Bad 5G signal
RSSI -51

08:39:18 AM Associated with 9F_906_meetingRoom
RSSI -52

Client switch to 9F_RD_03 (Client disconnect)

Table below displays client leave patterns when client leaves each connection session.

| Leaving reason | Description |
|---|---|
| **Incorrect password** | Client entered the incorrect password for WPA or wrong authentication information for EAP |
| **Client switch to {device_name}/{radio}** | When the RSSI signal is not good enough, the client did not disassociated from the AP and it connected to new AP directly with regular authentication procedure. |
| **Roam out to {device_name}** | When the RSSI signal is not good enough. The client disconnected from the original AP and connected to the new AP by 802.11r fast roaming protocol. |
|  | The client disconnected from the AP due to band |

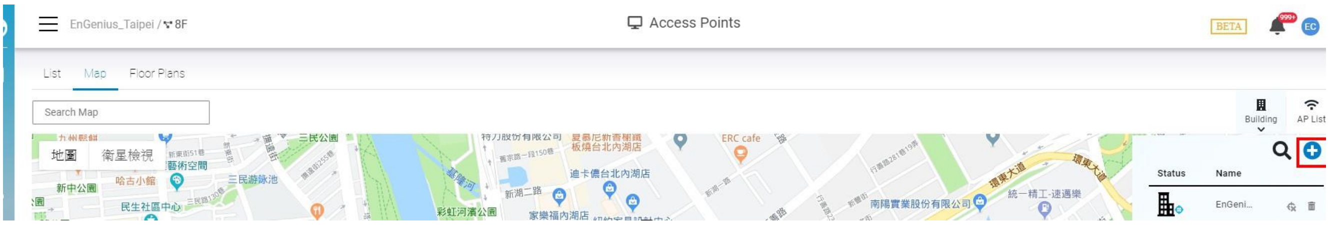
| | |
|---|---|
| **Steer to {radio}** | steering protocol. It received the 802.11v trigger and connected to suggested band accordingly. |
| **Disconnected by {device_name}** | The client was disconnected by the AP due to ba RSSI signal (fast handover). |
| **AP disconnect** | The client was disconnected by the AP due to unknown reason. |
| **Kicked by Cloud** | The client was kicked by the cloud administrator. |
| **Denied by ACL** | The connection was refused by AP because the client was on the blocked list under access contro |
| **Exceed client limit** | The connection was refused because the client count has exceeded the maximum 2.4G/5G client limit. |
| **Client inactive** | The client was inactive because it was on power saving mode or far away from the AP. |
| **Client disconnect** | The client disconnected because the user disable the Wi-Fi or choose to connect to other AP. |
| **Disconnected due to SSID configuration change** | The clients was disconnected due to SSID configuration change. Some configuration change took effect only after recycled (down&up) the NIC (network interface controller). When the NIC is down, all connection are disconnected. |

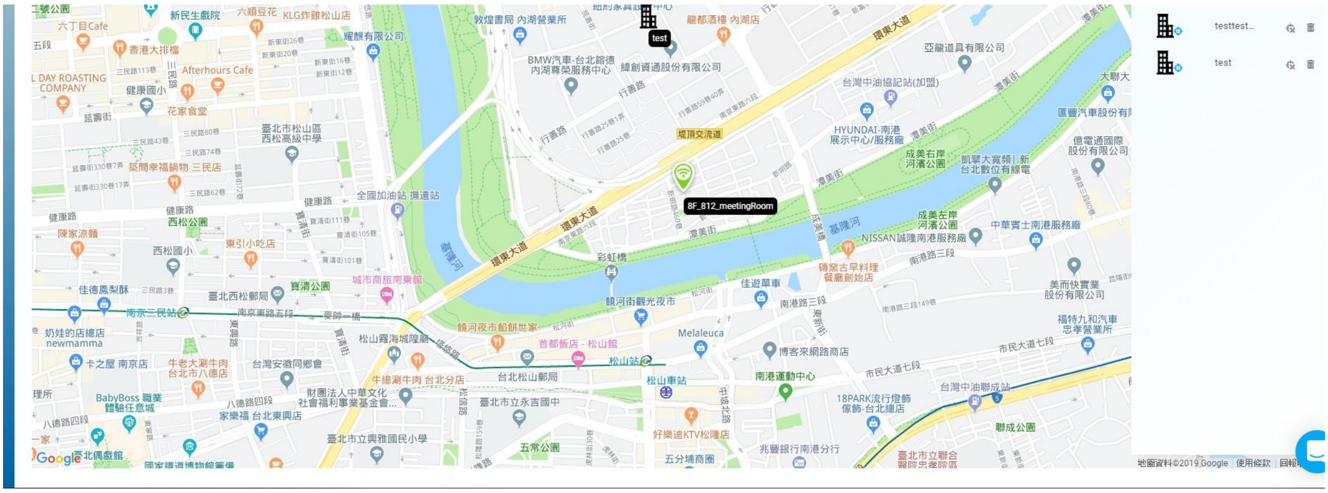
## Device Map Location

This screen allows you to locate a device on the world map to show the relationship between the space and EnGenius Devices. Maps provide a visualization for buildings and access points.

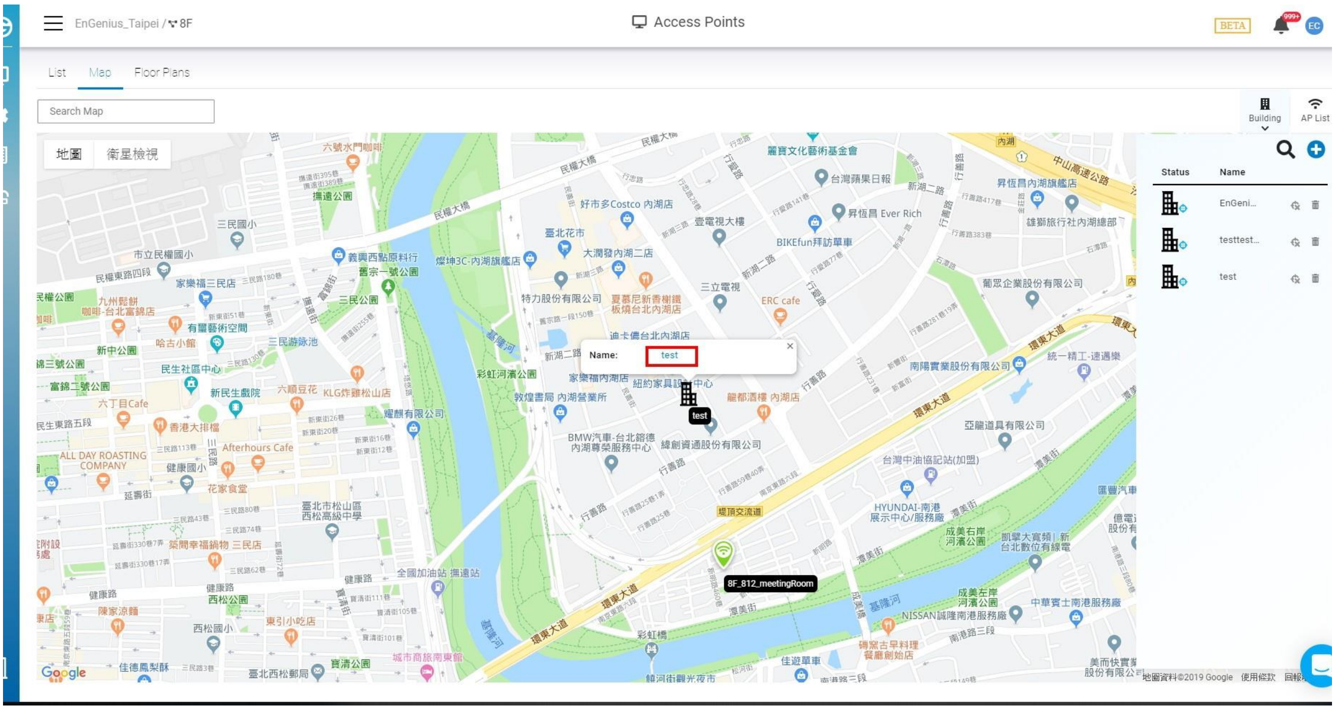
## Create Buildings

A **building** means a group of floor plans. You can create a new building with the **+** button.



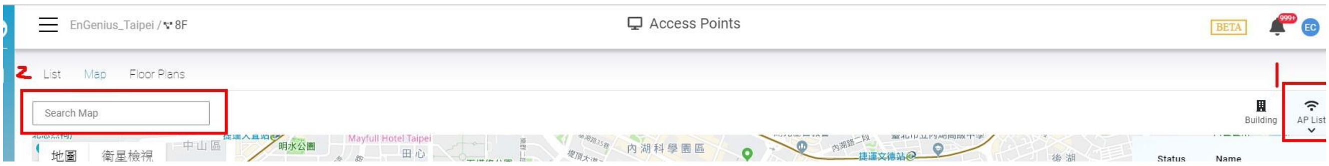


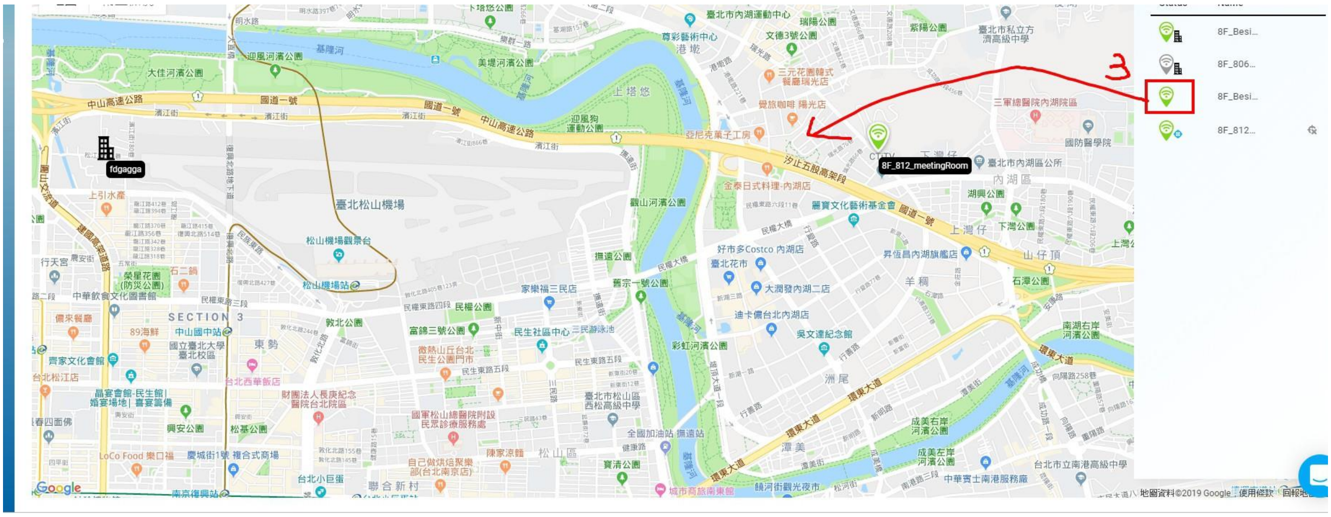
After you create a building, you can drag it to the map. Single-click on the building icon and a hyperlink will appear to allow you to edit floor plans.



## How to Place Access Points or Buildings on the Map

1. Click access point list or buildings list.
2. Enter the street address in the address field.
3. Drag the access point/building onto the map.

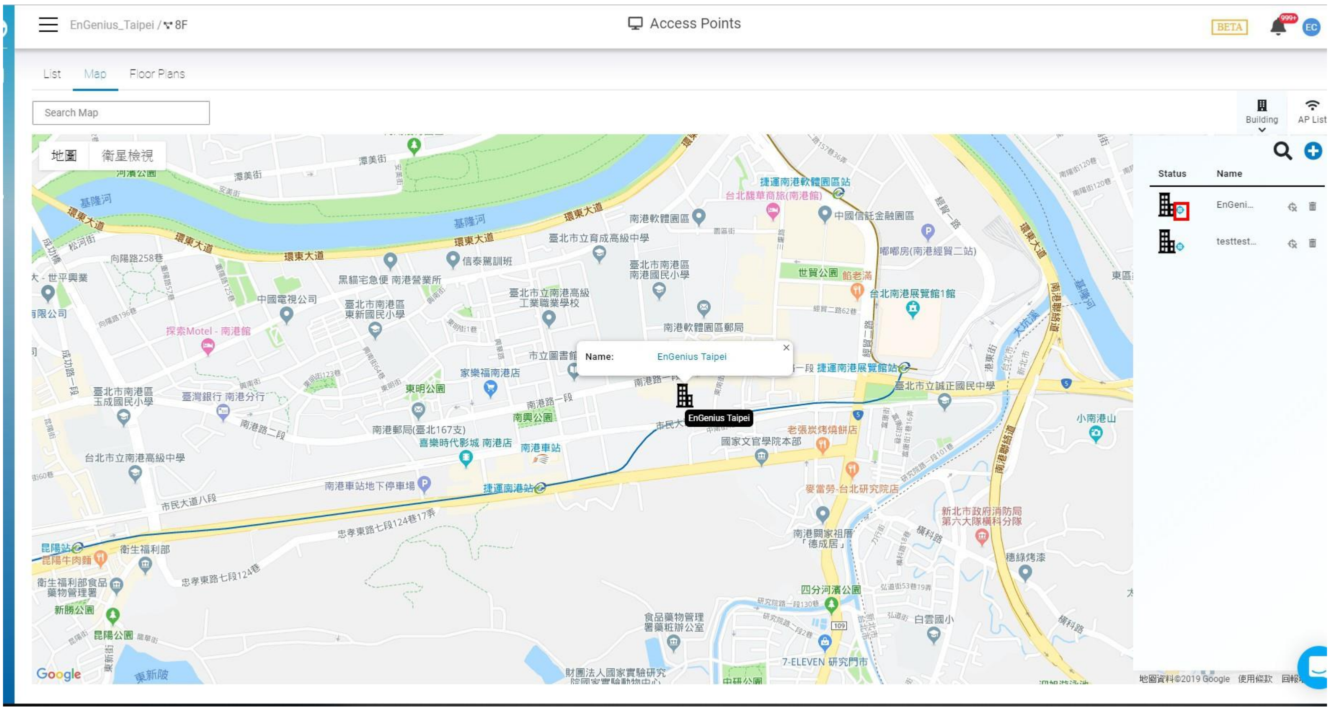


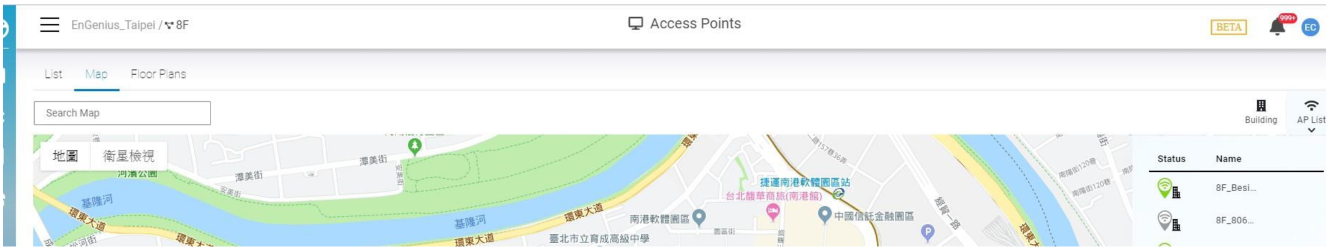


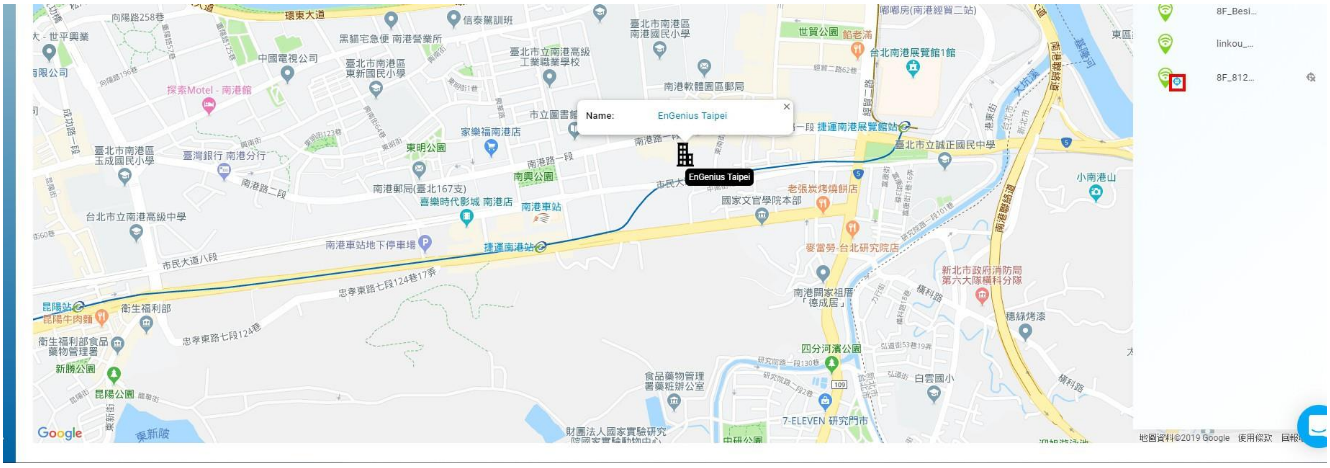
## Navigation

There are a number of ways to navigate through the map display.

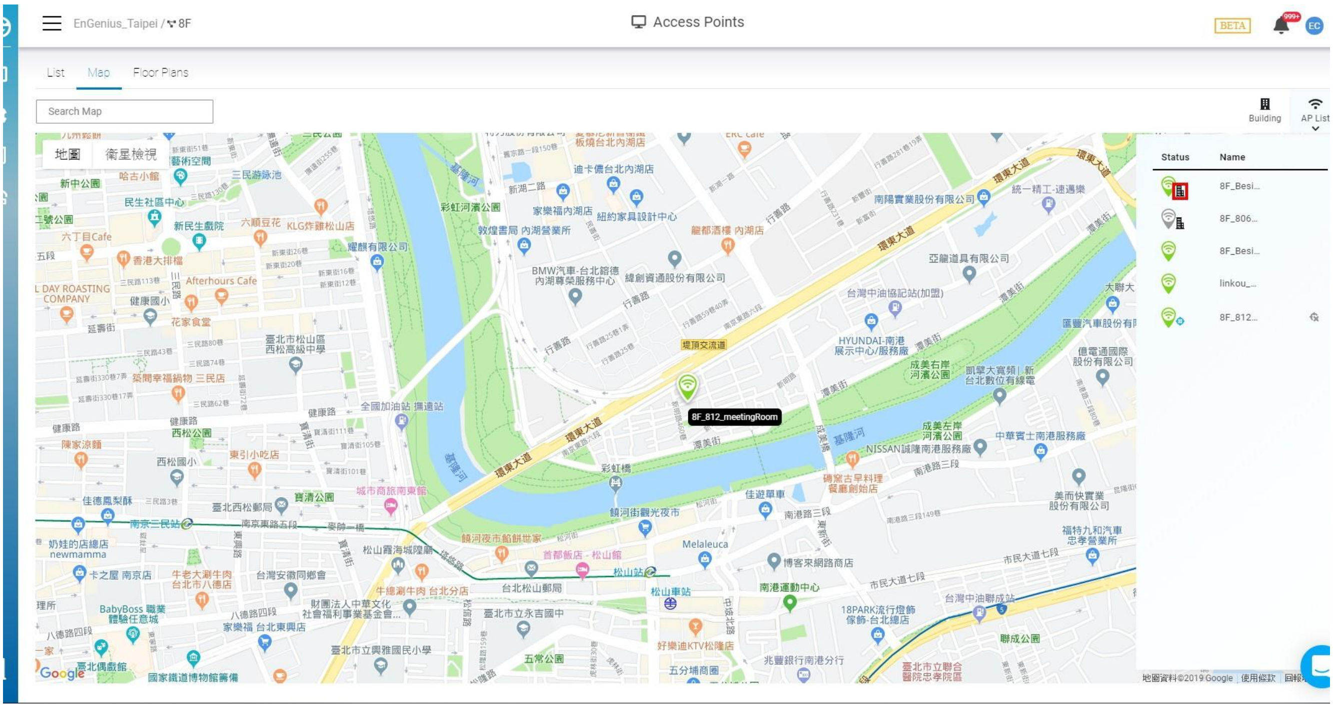
**Single Click**: If the user single-clicks on the focus icon on the access point or building lists, it will auto-locate the same item in the map.







**Double Click**: If the user double-clicks on the building icon in the access point list, the UI will auto-navigate to the floor plans of that building.



## Floor Plans

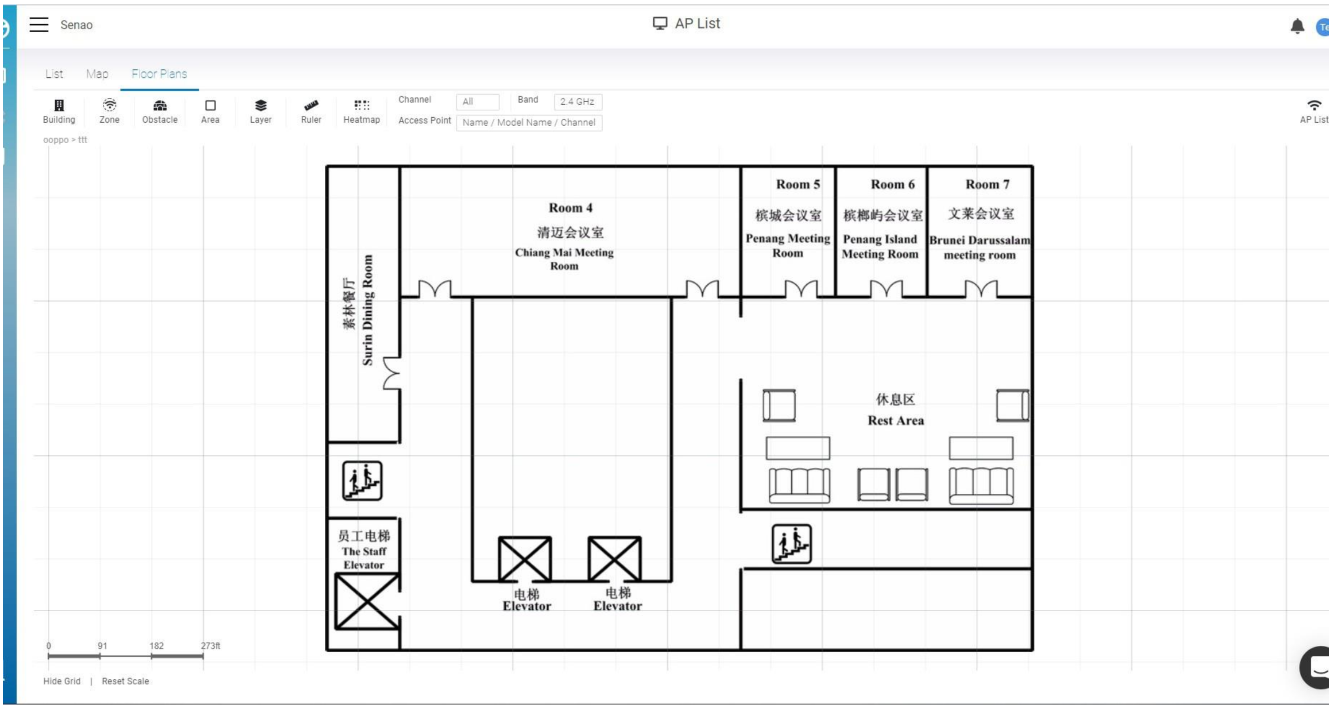
Floor plans allow you to simulate the heatmap. This article will discuss how to upload custom floor plans, pin them on the map, and place devices within these floor plans.

## Uploading Floor Plans

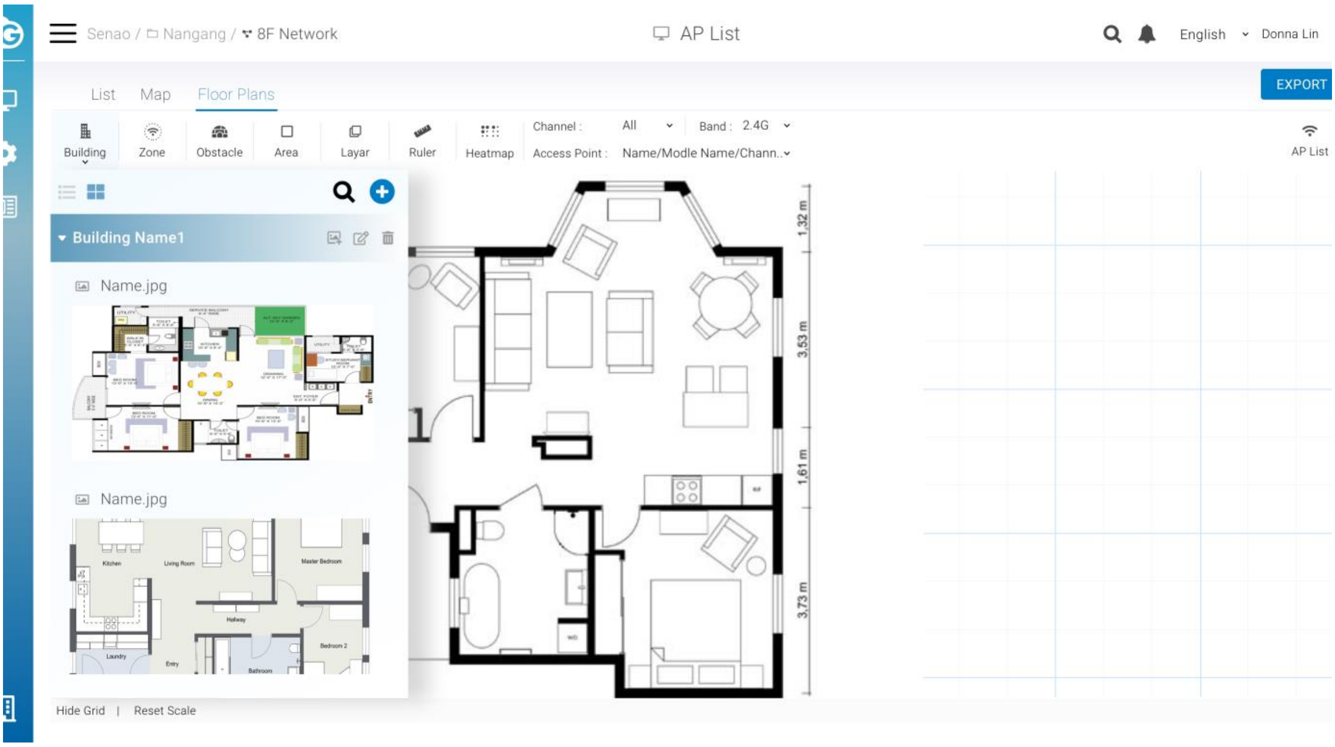
Before uploading floor plans, a building must be created to contain them (see **Managing Devices > Device Map Location** in the user manual).

To upload a custom floor plan/map**:**

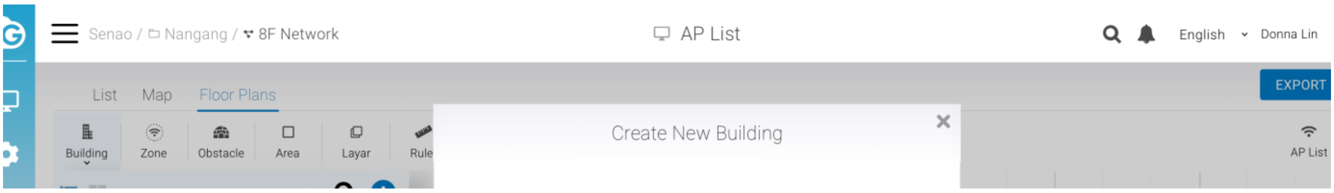
1. Navigate to **Manage > Map & Floor plans**.

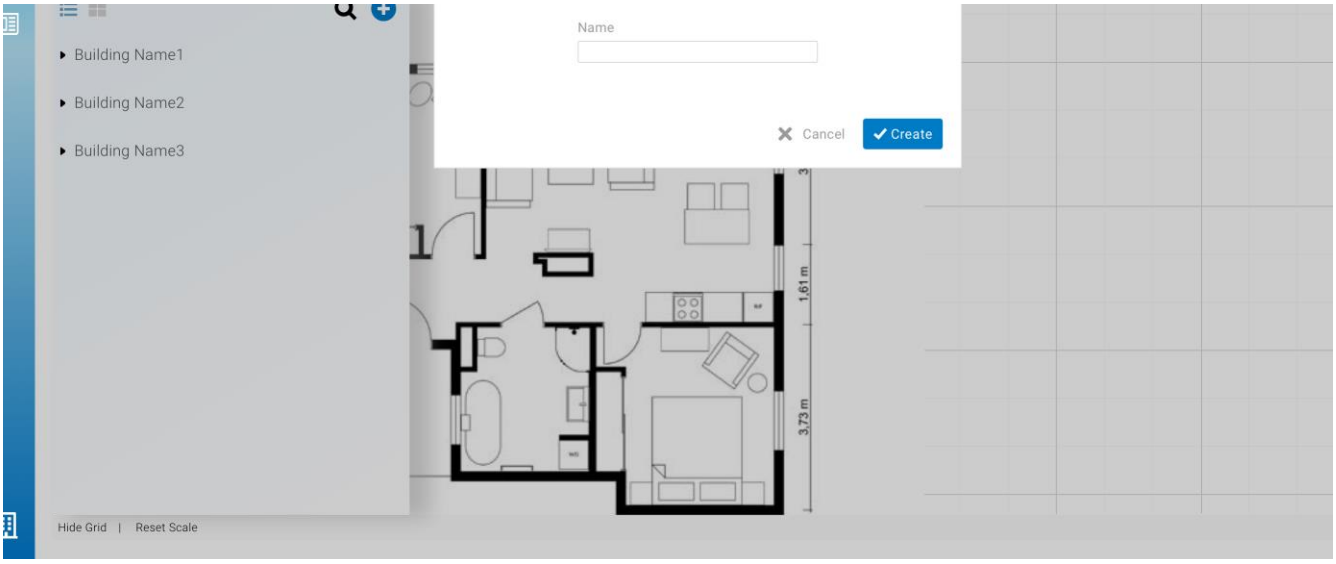


2. Click **Building** and click **Add**.

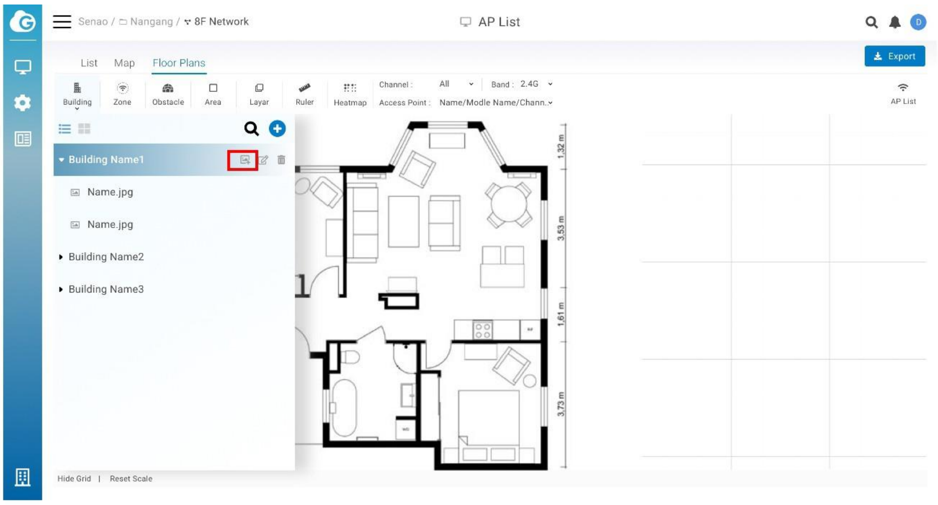


3. Enter a **name** and then click **Create**.

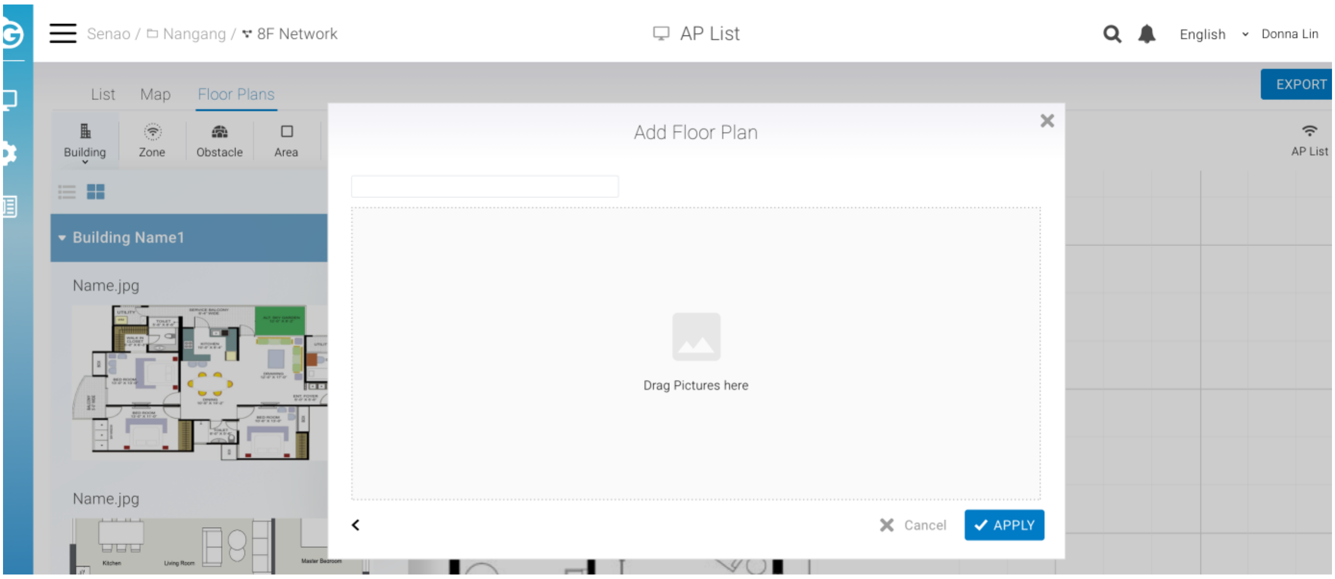


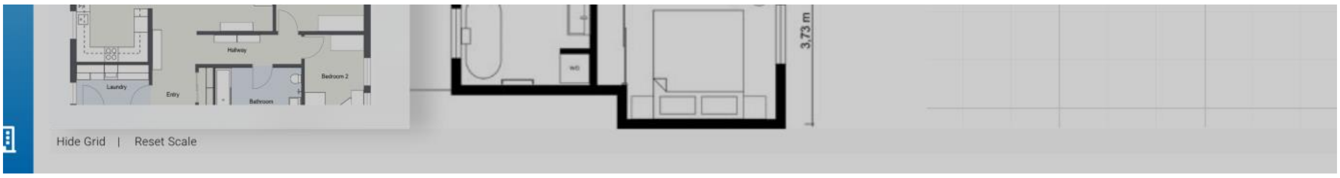


4. Find the building you have just created in the building list and click the picture icon**.**



5. Enter a **name** and upload the floor plan, then click **Apply**.



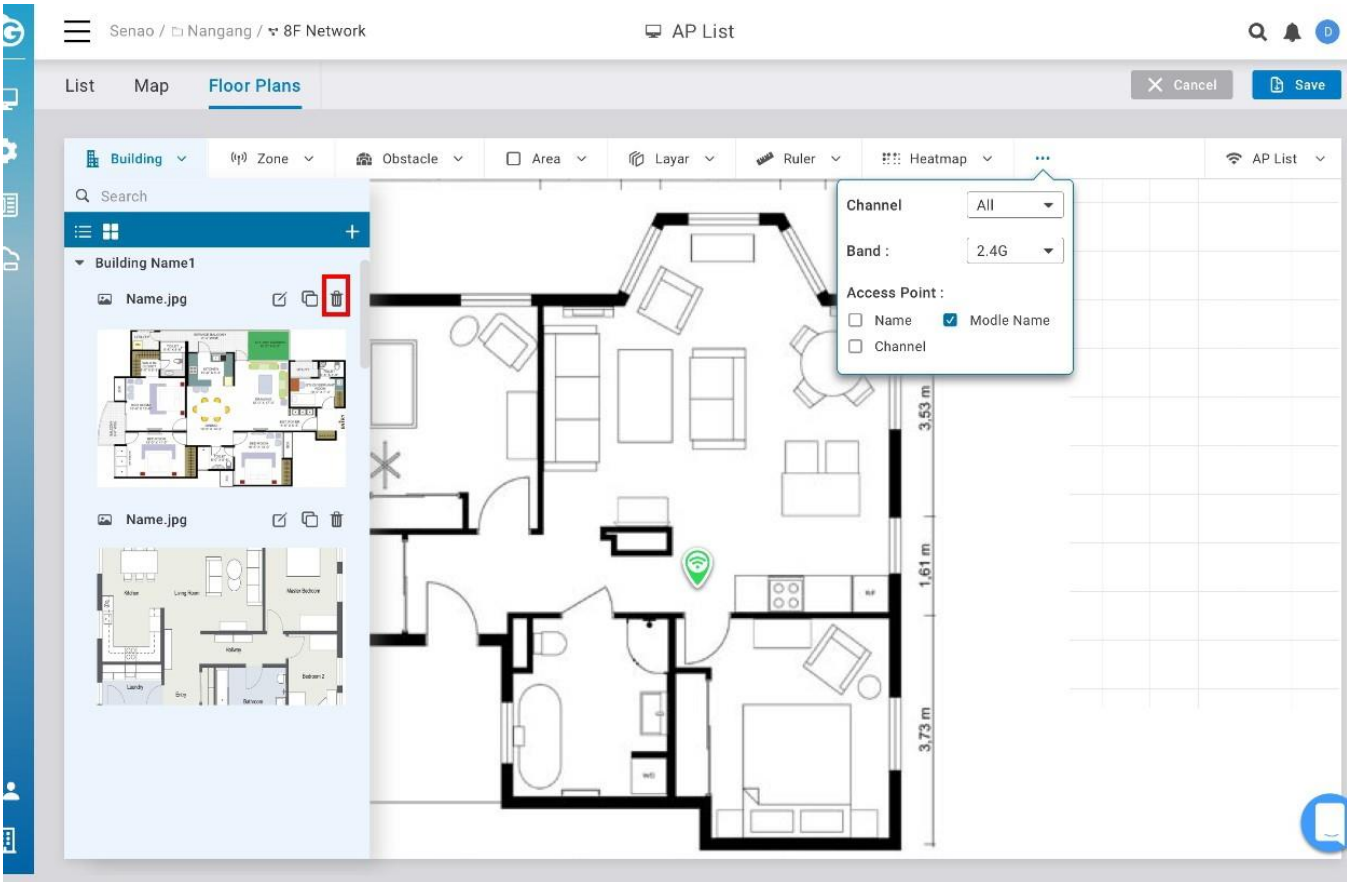


## Deleting a Floor Plan

If you no longer use a floor plan that you previously imported, you can delete it.

Follow these steps to delete a floor plan:

1. Find the building you created in the building list.
2. When the floor plan appears, hover over it and click **Delete**.



Channel: All

Band : 2.4G

Access Point :

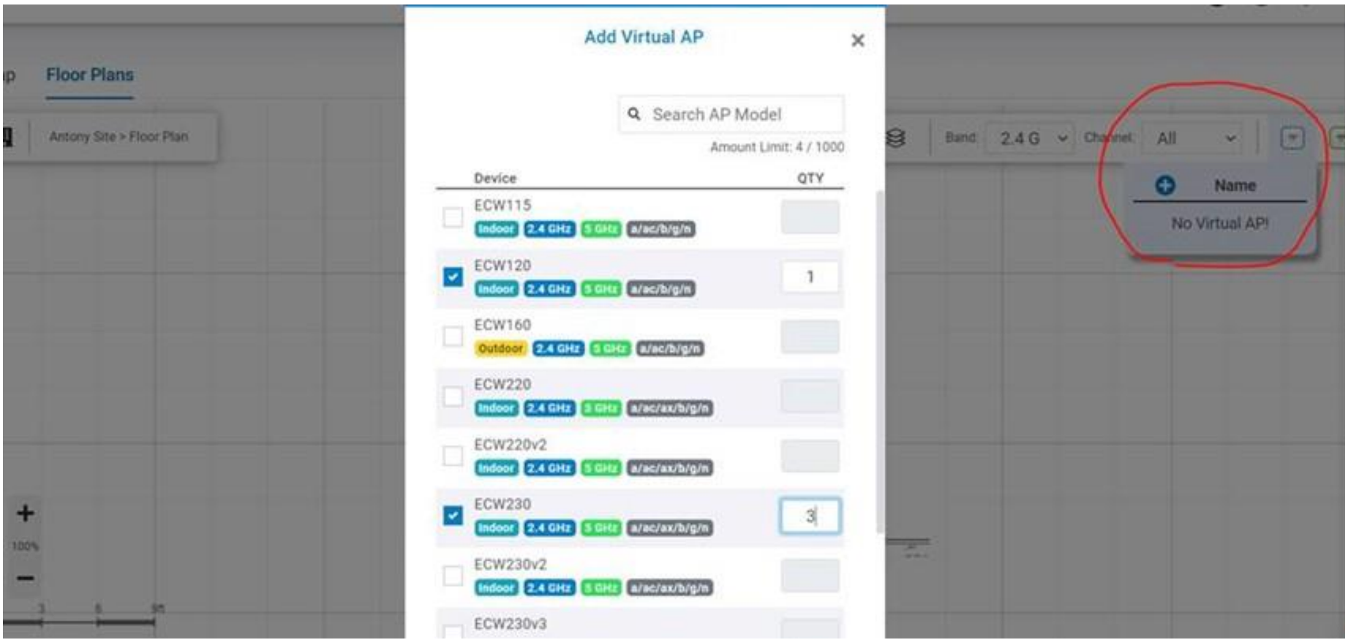
☐ Name ☑ Modle Name

☐ Channel

## Virtual AP

Virtual AP" is now available for users to add virtual AP together with "physical AP", so users can simulate the heat map if he adds more AP to increase the coverage

Add Virtual AP and choose units of models to add



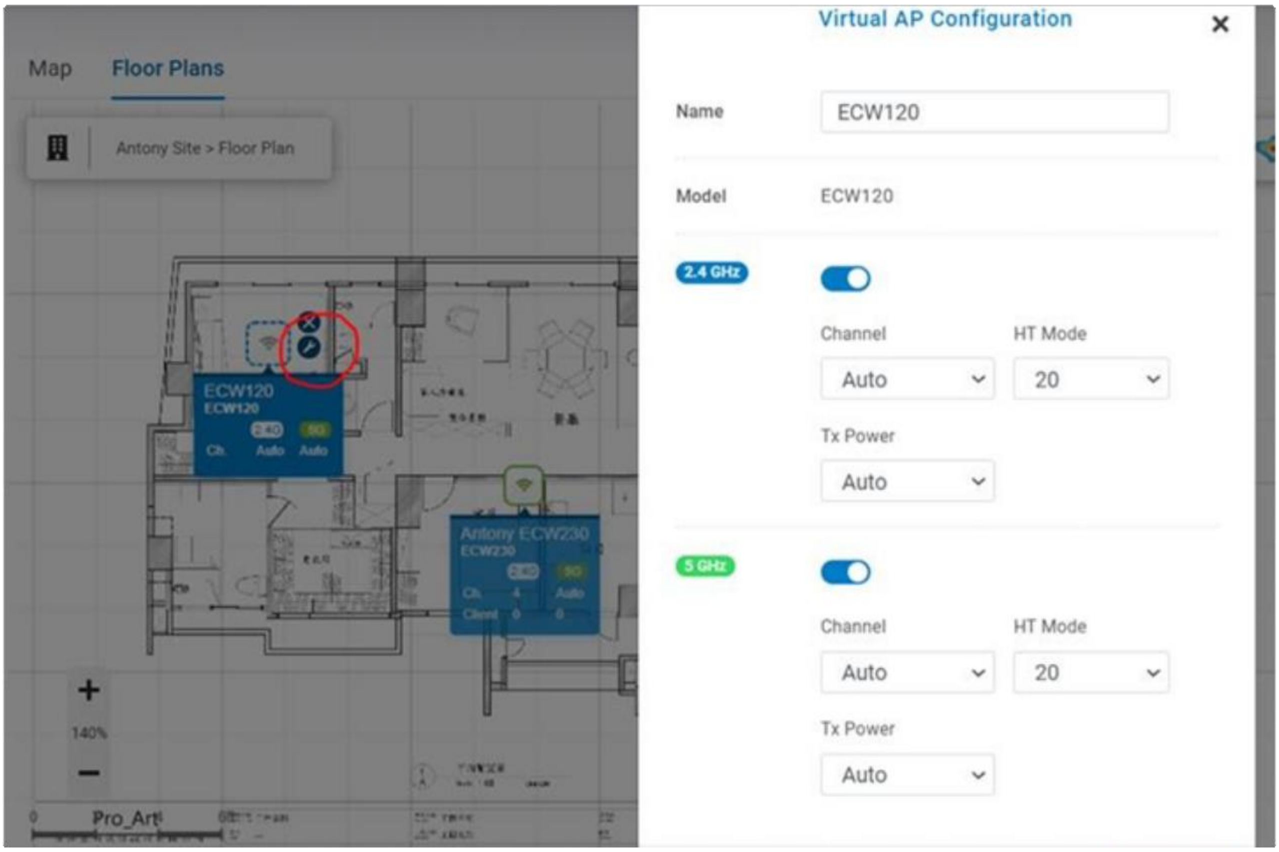
Add Virtual AP

Search AP Model

Amount Limit: 4 / 1000

| | Device | QTY |
|---|---|---|
| □ | ECW115<br>Indoor 2.4 GHz 5 GHz a/ac/b/g/n | |
| ☑ | ECW120<br>Indoor 2.4 GHz 5 GHz a/ac/b/g/n | 1 |
| □ | ECW160<br>Outdoor 2.4 GHz 5 GHz a/ac/b/g/n | |
| □ | ECW220<br>Indoor 2.4 GHz 5 GHz a/ac/ax/b/g/n | |
| □ | ECW220v2<br>Indoor 2.4 GHz 5 GHz a/ac/ax/b/g/n | |
| ☑ | ECW230<br>Indoor 2.4 GHz 5 GHz a/ac/ax/b/g/n | 3 |
| □ | ECW230v2<br>Indoor 2.4 GHz 5 GHz a/ac/ax/b/g/n | |
| □ | ECW230v3 | |

The Tool icon for users to modify the tx power and channel for heat map simulation



Virtual AP Configuration

Name: ECW120

Model: ECW120

2.4 GHz

Channel: Auto HT Mode: 20

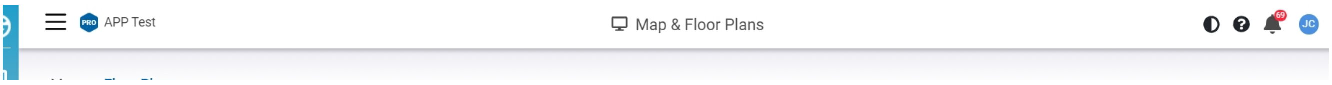
Tx Power: Auto

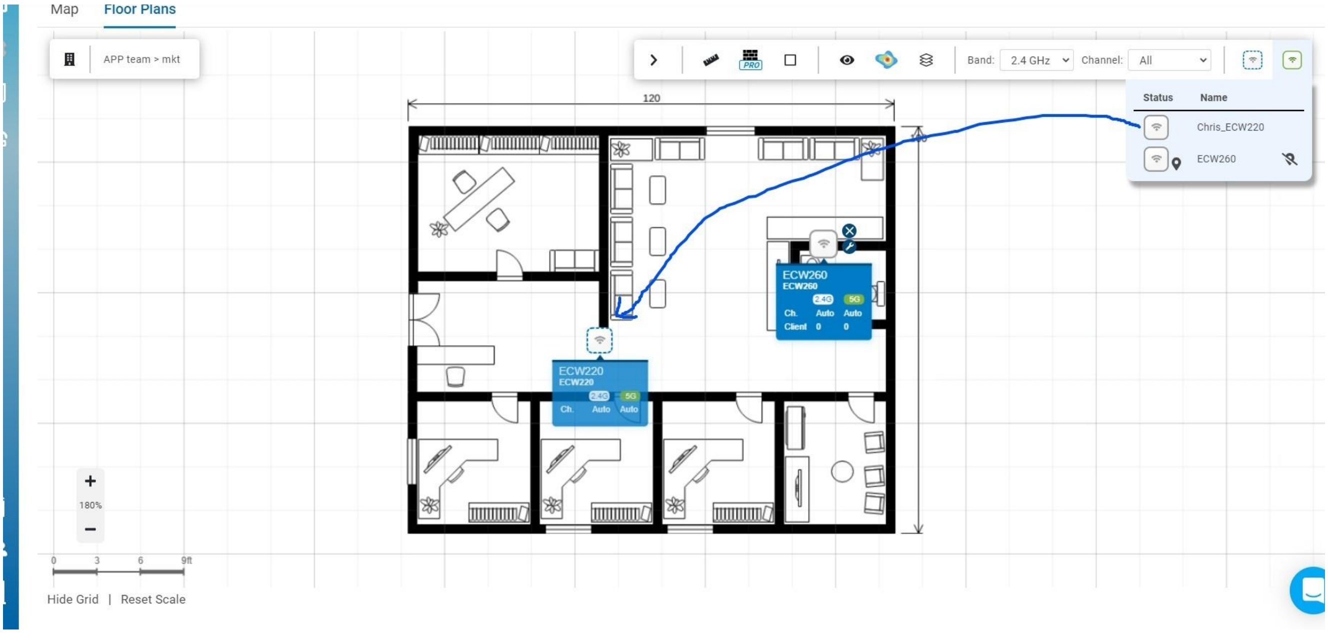
5 GHz

Channel: Auto HT Mode: 20

Tx Power: Auto

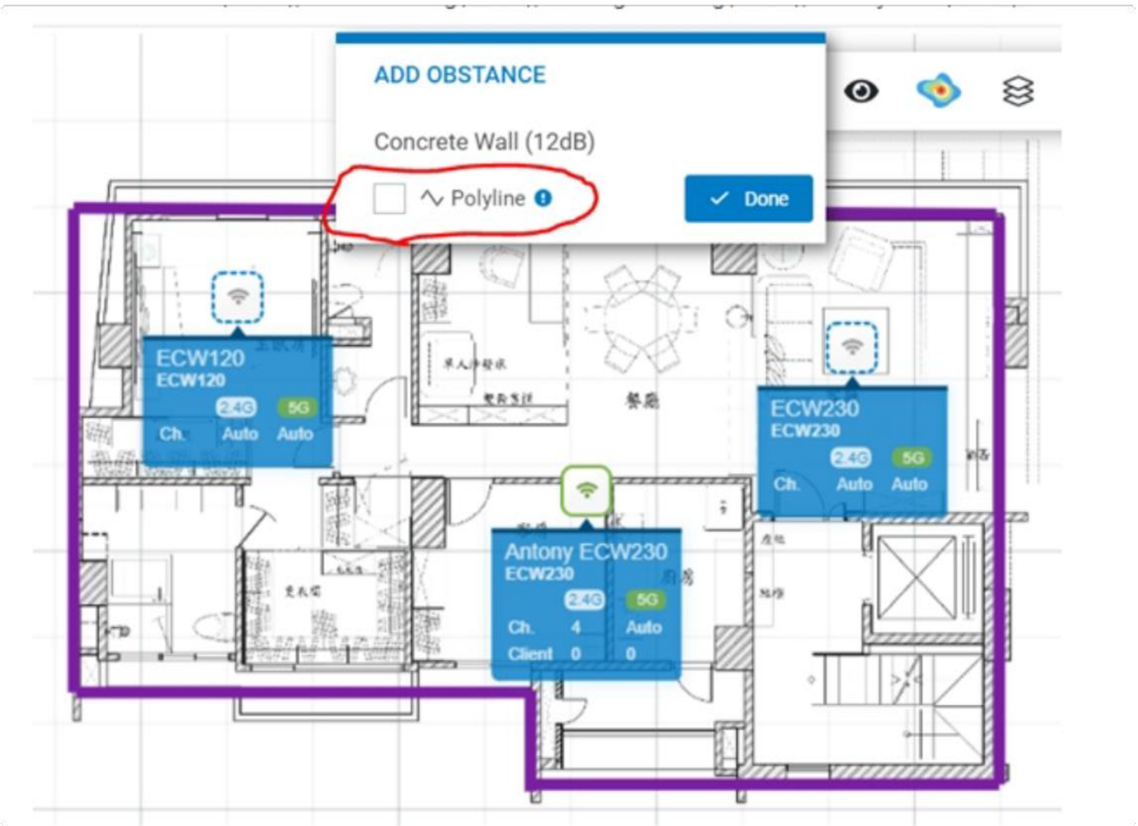
Drag the physical AP to Virtual AP (model needs to be the same) then physical AP could use the Virtual AP configuration.





## Polyline in Obstacle

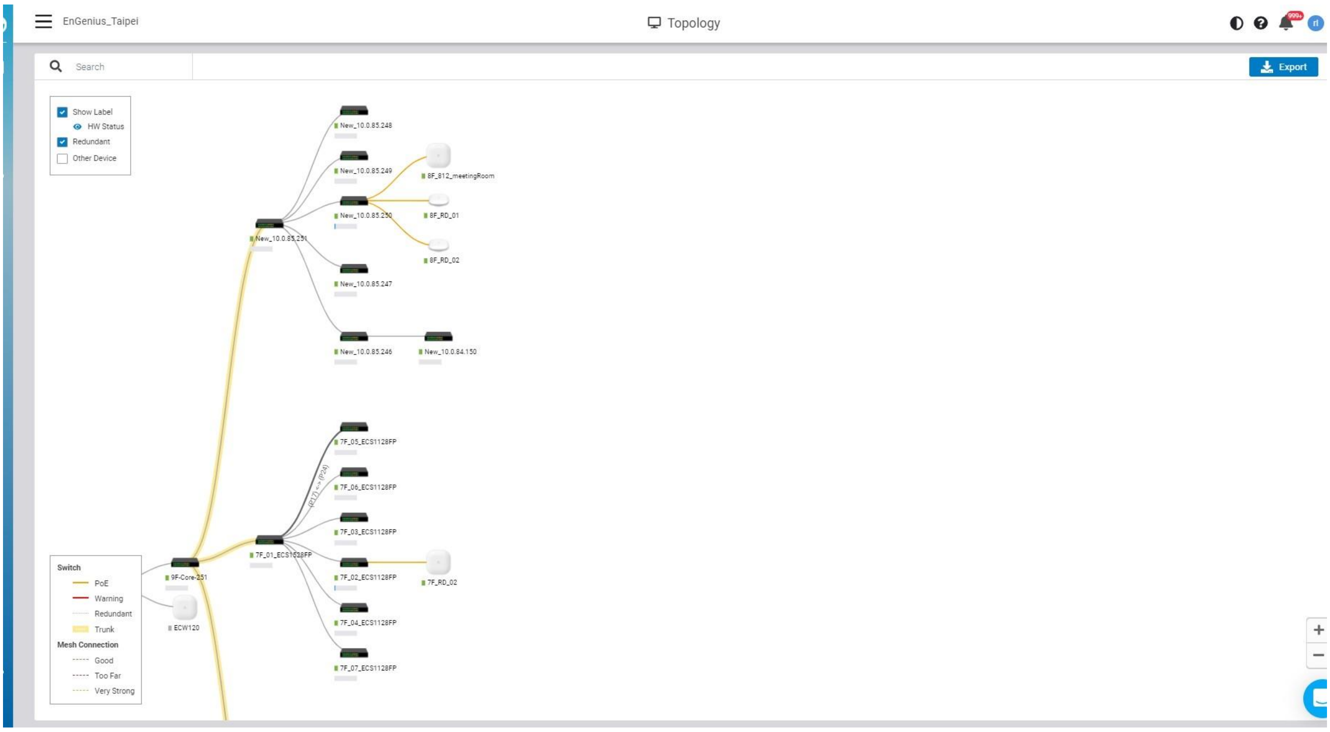
When drawing the walls, users used to draw the line one by one by click “start” and “end” for straight lines, now with the **“Polyline”** option available, users can simply click on the turning point to draw lines quicker.



# Topology

Network topology is a powerful tool to provide administrators a graphic overview of the logical network topology and the status of EnGenius devices.

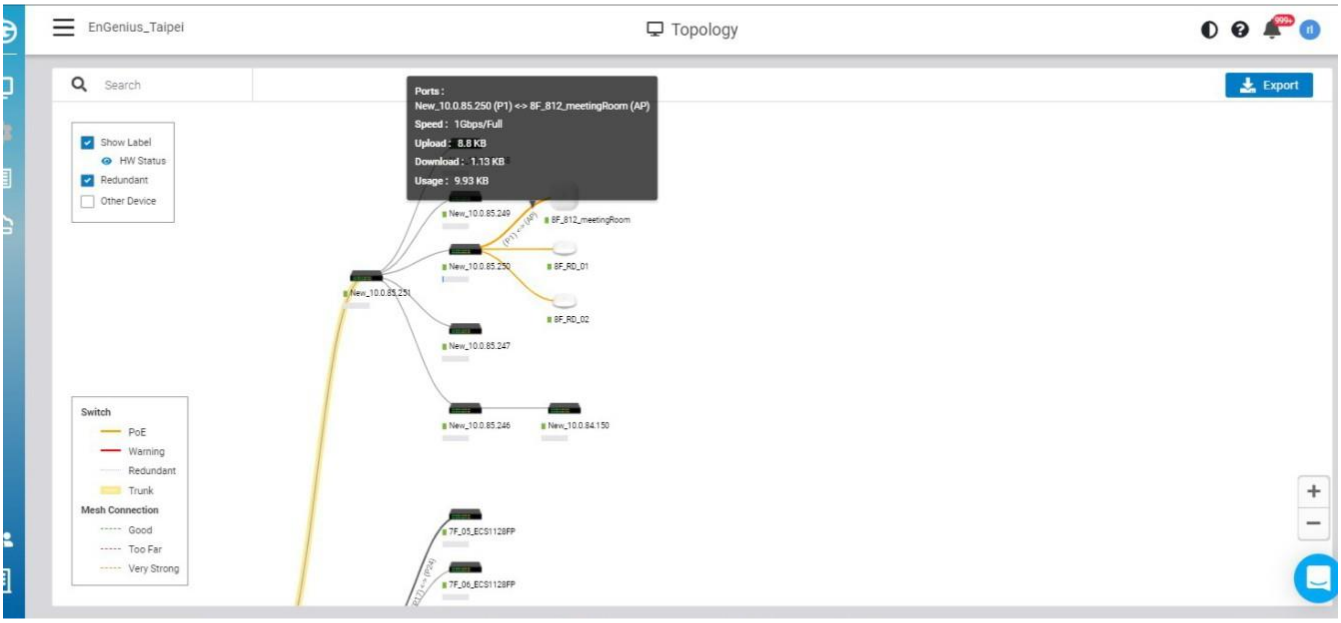
Use this screen to view the  topology of the Org/Network. Click **Manage** > **Topology** to access this screen and  double-click the organization/hierarchy view/network on the tree to change the scope.



☑ Show Label
HW Status
☑ Redundant
☐ Other Device

Switch
PoE
Warning
Redundant
Trunk
Mesh Connection
Good
Too Far
Very Strong

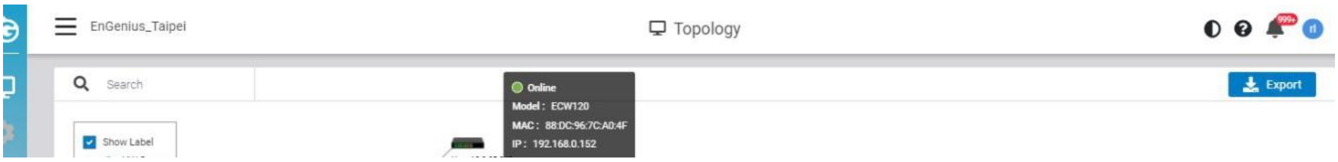
Learn which physical links in your network are most heavily-trafficked; simply hover over individual network links and devices to learn statistics about that connection's negotiated speed, usage, and a number of directly connected clients using it in the past 5 minutes.



Ports :
New_10.0.85.250 (P1) <-> 8F_812_meetingRoom (AP)
Speed : 1Gbps/Full
Upload : 8.8 KB
Download : 1.13 KB
Usage : 9.93 KB

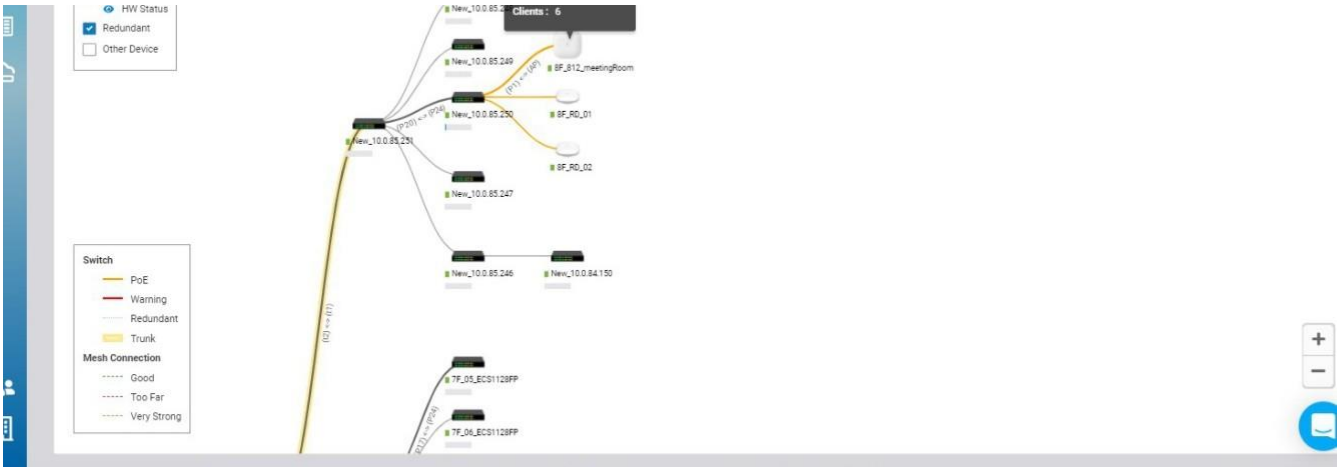
☑ Show Label
HW Status
☑ Redundant
☐ Other Device

Switch
PoE
Warning
Redundant
Trunk
Mesh Connection
Good
Too Far
Very Strong



● Online
Model : ECW120
MAC : 88:DC:96:7C:A0:4F
IP : 192.168.0.152

☑ Show Label



The following describes the functions on this screen:

**Show label** : Click to display or hide the device name & HW status on each device.

**HW status** : Click to display or hide the POE Utilization on each switch.

**Redundant** :  Click to display or hide the redundant link .

**Other Devices :** Click to display the third party devices as well as  EWS series devices.

**Export** : Click to download topology as PDF format .

## Configuring Networks

There’s a lot that EnGenius Cloud can do to customize a network to meet your specific needs. We’ll walk you through the most common settings here.

## Configuring SSIDs

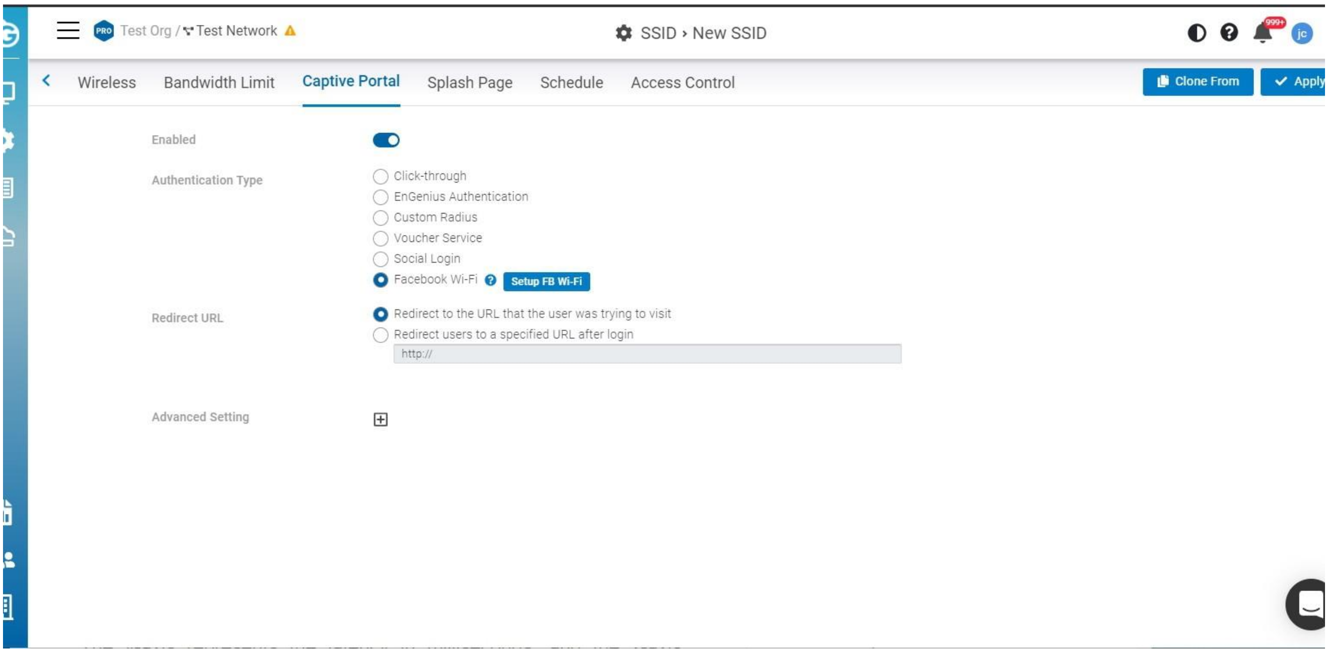
# Facebook Wi-Fi

Facebook login provides a social sign-on experience for users logging in to access points. You can use your Facebook page as the sign-in page when they first log in to your network. Users can then check in with their Facebook credentials, update their status, and 'like' the Facebook page.

## Configuring EnGenius Wi-Fi with Facebook Login

After creating a Facebook page, Facebook Login is configured on the **Configure** > **SSID** > Click one of the SSID > **Captive Portal** by taking the following step:

1. Select **Facebook Wi-Fi** under the **Authentication Type** section and click the **Setup Facebook Wi-Fi** button**:**



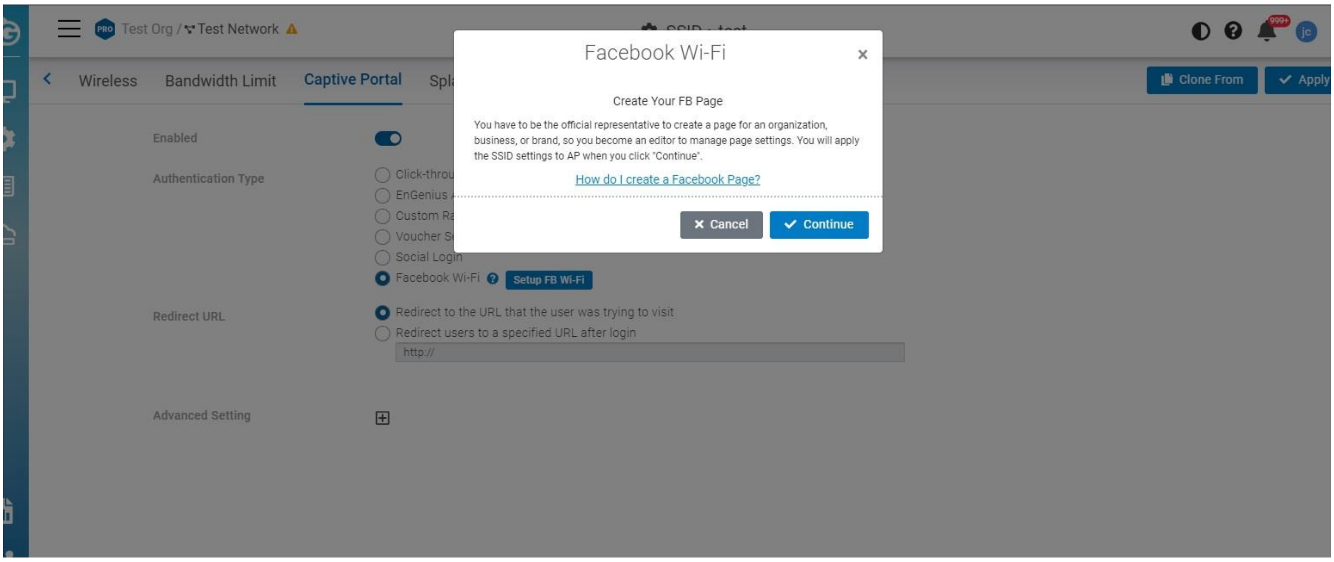
Enabled

Authentication Type
○ Click-through
○ EnGenius Authentication
○ Custom Radius
○ Voucher Service
○ Social Login
● Facebook Wi-Fi  Setup FB Wi-Fi

Redirect URL
● Redirect to the URL that the user was trying to visit
○ Redirect users to a specified URL after login
http://

Advanced Setting ⊞

2. Wizard is displayed. Click **Continue** if you have created the Facebook page in advance. If you haven't created it, you could create a Facebook page.



Facebook Wi-Fi

Create Your FB Page

You have to be the official representative to create a page for an organization, business, or brand, so you become an editor to manage page settings. You will apply the SSID settings to AP when you click "Continue".

How do I create a Facebook Page?

Enabled

Authentication Type
○ Click-throu
○ EnGenius
○ Custom Ra
○ Voucher S
○ Social Login
● Facebook Wi-Fi  Setup FB Wi-Fi

Redirect URL
● Redirect to the URL that the user was trying to visit
○ Redirect users to a specified URL after login
http://

Advanced Setting ⊞